Rights & Democracy
International Centre for Human Rights
and Democratic Development

1100-1001, de Maisonneuve Blvd. East, Montreal, H2L4P9, Canada
www.ichrdd.ca ichrdd@ichrdd.ca

SUMMARY OF CANADA'S TRADE PROMOTION AND HUMAN RIGHTS ACTIVITIES IN CHINA

Overall Trade with China : A Growing Market

The People's Republic of China (excluding Hong Kong) is Canada's fourth largest export market (after the US, the EU and Japan). In 2000, Canada's total exports to China totaled $3.7 billion (an increase of 39.3 % over 1999) and imports were worth $11.3 billion, an increase of 26.4 % over 1999. A promising and growing market which Canada's Export Development Corporation (EDC) refers to as : « Asia's only decent demand story ». China is also the secondlargest destination of foreign direct investment in the world, including $420 million from Canada in 1999 (up from $257 million in 1994, but compared to $3 billion in HK)). Canada is looking towards the negotiation of a bilateral investment protection agreement with China (a FIPA or Foreign Investment Protection Agreement).

Diplomacy : Economic Interests at Top of Canadian Agenda

Diplomatically, China is considered a very important country for Canada. This is not surprising given that China accounts for almost a quarter of the world's population, in addition to many other factors (history, immigation, cultural ties etc). As such, substantial resources are devoted to strengthening the relationship. For example, from 1998-2000, no less than 20 Ministerial visits took place including visits by the Prime Minister, Ministers of International Trade, Finance, Foreign Affairs, Defence, Industry, Agriculture, Natural Resources, Immigration, Public Works, National Revenue as well as Secretaries of State for Asia Pacific and Science and Technology. Several other high-profile figues visited China including the leader of the opposition, the head of the armed forces and the Chief Justice. Senior Chinese officials have also made many visits to Canada.

There are a variety of issues that have been pursued on these visits, but the real heart of the matter, as shown the the portfolios of the Ministers who have been, is increasing Canada's economic ties with China. The problem is not so much that Canada has increased trade with China*; the problem is that while trade is receiving a lot of attention, human rights seem to have fallen to the bottom of our list of priorities.*. Chinese citizens who are bravely fighting for human rights -- for democracy, for freedom of speech, for workers' rights, indeed for their rights to life, liberty and security of the person -- are finding that their rights are being sacrificed by Western governments who are in a race to get a foothold in the competitive Chinese market.

The consistent and deplorable decline in diplomatic support for the resolution on human rights in China at the annual UN Commission on Human Rights coincides with increased Western economic interests in the country and quite explict warnings from the Chinese to not « meddle » in « internal matters ».

Canadian Government and Canadian Business in China

Team Canada as most visible manifestation of Canadian government interest in Chinese market with Feb 2001 edition including the Prime Minister, 8 premiers, 3 territorial leaders and 800 businesses, « providing the Canadian business community with an incredible degree of government support » (according to the Canada-China Business Council). In fact however, the Canadian government is busy in a myriad of ways promoting increased trade and investment with China. Compare the resources that are devoted to trade with those devoted to human rights :

Trade	Human Rights
Close ties between the Canadian Embassy in Beijing and Canadian business in China. Ex.: Former Canadian ambassador to China Howard Balloch is now President of the Canada-China Business Council. Business community has political leaders regularly acting on their behalf. Web page full of information that is useful for business.	Human rights are such a low priority that the Prime Minister receives kudos simply for mentioning them in a speech! There is no sustained or substantive policy dialogue between human rights NGOs and the government on China.
Hundreds of officials in DFAIT headquarters, other departments, embassies and consulates devoted to increasing trade with China and helping Canadian businesses establish themselves. Detailed sectoral briefings, business contacts and advice all in a days work.	The entire human rights team of DFAIT consists of 20 officials and there is no single person devoted to questions of human rights in China. No comparable assistance offered to human rights groups working on China.
The Canadian government issues regular market research reports made available free of charge to companies interested in investing or trading with China, which supply up-to-date information on latest market trends and regulations as well as contacts in both China and Canada that can be of assistance. In the last two years over 30 market reports have been developed on aerospace and defence; agriculture, food and beverages; arts and cultural industries; automobiles; building products; electric power equipment and services; environmental industries; forestry; health industries; information and communication technologies; metal, minerals and related equipment; oil and gas; rail and urban transit; services; space industries.	There is very little public information available on Canada's position on human rights in China. The reports on human rights in China done by the Canadian government are confidential (as they are on all other countries). A two-page description of human rights in China is generally distributed prior to the NGO consultations on human rights held in early spring. Occasionally a press release by a Minister is put out, or timid comments about human rights will be found in speeches. The much-touted bilateral dialogue on human rights in China has virtually no paper trail.
Financing support and insurance including political risk insurance through several different government agencies, notably the Export Development Corporation, the Canadian Commercial Corporation and CIDA Inc. It is impossible to get precise figures on what projects have been supported through public funds. EDC support to the advanced information and telecommunications sector in China since 1995 is $841,884,442.32.	CIDA does have some bilateral projects on human rights in China related to judicial reform and other matters, all of which require the cooperation of the Chinese government. Estimated total for year 2000 : $11 million.
Face-to-face briefings by embassy staff to anyone who requests it two weeks in advance.	No such arrangement available for those seeking information on human rights in China.
The telecommunications and information technology sectoral advisory group on international trade (SAGIT) which advises the Minister of International Trade on what Canadian business want from international trade negotiations is uniquely composed of representatives of the business sector.	Human rights NGOs are invited once a year to put forward recommendations on human rights in China at an annual 2-3 day consultation dealing with all countries and issues globally. No human rights groups officially advice Canada on its trading relationship with China.
Substantial resources are devoted to favourable multilateral trade rules including strong support for Chinese accession to the World Trade Organization, for the Information Technology Agreement (ITA) and for the Agreement on Basic elecommunications under the GATS (General Agreement on Trade in Services).	Canada, along with many other Western countries has jettisoned the multilateral system of human rights protection in favour of a bilateral dialogue with highly questionable results.

What About the Telecommunications/Information Technology Sector?

- The Canadian Embassy in Beijing issues a newsletter on developments in this sector, providing advise to Canadian corporations and up-to-date legal and market information.

- Over the past five years, in the field of advanced technologies and telecommunications, the Export Development Corporation has provided $841,884,442.32 in short-term and medium-long term financing which includes short-term domestic and export insurance as well as political risk insurance, contract insurance and bonding and financing. There is no process for screening the end uses to which technology exports supported by EDC will be used. Some projects in China have reportedly been turned down because they were considered unsuitable on human rights or environmental grounds but EDC will not release a detailed breakdown on what projects have received financing or insurance, despite its new and improved disclosure policy which entered into force on Oct. 1, 2001.

- The Bank of China is one of EDC's prime borrowers in China. EDC also has relationships and memorandums of understanding with the State Development Bank of China, the Export-Import Bank of China and the Industrial and Commercial Bank of China, all owned by the Government of China.

- John Roth, former CEO of Nortel, on EDC: "My only input would be: Don't change it too much. If it's not broken, don't fix it."

- Between 1992 and 1998, Nortel donated $357,447.04 to the Liberal Party of Canada.

Review of China's Internet Regulations and Domestic Legislation

China's Internet regulations and legislation are guided by the principle of "guarded openness" - seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination, and the use of the Internet by domestic or foreign groups to coordinate anti-regime activity. While researchers often refer to a national Internet strategy, there is in reality, no single "official" articulated strategy, written down and approved by the Chinese leadership. The research here is therefore, an aggregation of the interrelated Internet security policies and regulations pursued by the various bureaucracies.

In China, the security apparatus includes all those organizations responsible for internal or external security. The two most important are the Public Security Bureau (PSB), which is responsible for internal security, and the Ministry of State Security (MSS), which handles foreign civilian intelligence-gathering and internal counter-intelligence against foreign threats.

As China modernizes its telecommunications infrastructure, both organizations have evolved corresponding claims to regulating Internet security – the global character of the Internet makes it difficult to define the distinction between internal and external security.

The stakes are high – for the government, as China integrates into the global economy, and for the would-be "cyber-dissident", who ultimately faces the death penalty for illegal use of the Internet. The bureaucratic environment for information security is very complicated, characterized by on-going struggles over jurisdiction and authority.

The Public Security Bureau

The Public Security Bureau is in charge of maintaining China's civilian network security, both physical and on-line. The primary PSB unit charged with maintaining network security is the Computer Management and Supervision Bureau, which was founded as early as 1983. Its responsibilities are formally codified in *"Computer Information Network and Internet Security, Protection and Management Regulations,"* which was approved by the State Council on December 11, 1997.

Under the 1997 regulations, the PSB is tasked with oversight of Internet Service Providers and all other commercial enterprises that have users with Internet access. According to Article 8, "units and individuals engaged in Internet business must accept the security supervision, inspection, and guidance of the Public Security Bureau." The PSB requires Internet companies to provide monthly reports on number of users, number of page views, and user profiles. ISPs are also required to assist the Public Security Bureau in investigating incidents involving law violations and criminal activities involving computer information networks. Like network security, responsibility for maintaining security lies with the ISPs, and violations by users will result in the cancellation of the ISP's business license and its network registration, fines, and possible criminal prosecution of both the company staff and the user (Articles 20-23).

In the past year the Chinese government has rapidly built-up a legal framework on the foundation of the 1997 regulations. In less than one year, no fewer than three laws were passed, all of them extensive.

Legislation passed on October 1, 2000, deals with the involvement of foreign investments in the Internet sector and the control that operators have over their sites. It requires that any foreign companies wishing to invest in this sector obtain an authorization from the Ministry of the Information Industry. In addition, managers of Chinese sites are responsible for editing and censoring the content published on their sites, and, if not, risk fines or closings.

One significant new aspect of the law is that they are now required to report any infractions to the proper authorities. They must also be able to provide the authorities with the addresses of Internet users who have visited their site in the past sixty days. This new regulation also reinforces the prohibition of any "subversive" information on the Internet, particularly documents which incite "ethnic hatred, discrimination, feudal superstitions", spread "rumours that could lead to social disorder or damage social stability", advocate Tibetan or Taiwanese independence, or have content containing "obscenity, pornography, violence or terrorism".

Important legislation was implemented on November 6, 2000, concerning the content of news sites and Chinese discussion forums. It specifies that sites can only publish information provided by public media, that is, content which has undergone censorship within the constraints of official state propaganda. News originating from foreign media sources can no longer be published on Chinese sites unless an official authorization has been obtained. In addition, web sites are held responsible for any "subversive" information they publish. These measures also concern discussion forums. Anyone who violates this new law, especially those responsible for web sites, face administrative sanctions, fines, or prison sentences, depending on the "seriousness" of their wrongdoing. This measure means that news portals, such as Sohu.com are now wholly dependent on China's official press.

On December 28, 2000 a law was passed stating that "spreading rumours, defamation or publishing harmful information, inciting the overthrow of the country's government, the socialist system or a division of the country" is now considered "cyber-crime" and "cyber-dissidence". It provides for prison sentences for "the promotion or organization of religious cults" and "leaking State secrets". In January 2001, the official news agency Xinhua announced that anyone involved in "espionage activities" such as "stealing, uncovering, purchasing or disclosing State secrets" using the web or by other means, risks the death penalty, or from ten years to life in prison.

The Ministry of State Security

The Ministry of State Security (MSS) is responsible for external civilian intelligence-gathering and internal counter-intelligence. The MSS was formed in June 1983, combining the external intelligence, counter-intelligence, and internal security functions

of the PSB and the *"Investigation Department of the Chinese Communist Party Central Committee"*. The MSS has been locked in an on-going bureaucratic struggle with the Ministry of Public Security ever since. The bureaucratic competition between the PSB and the MSS is most acute in the area of information security, where the distinction between external and internal security is unavoidably opaque.

The MSS has the clear mandate to thwart foreign efforts at undermining Chinese information security, but this frequently intersects with the PSB's role, for example, in domestic network security. Similarly, the MSS feels it has a monopoly on undermining overseas subversion plans, particularly in Tibet and Xinjiang, but the PSB oversees Internet Service Providers and other facilitators of contact with the outside. As a result, the two bureaucracies remain mired in a cycle of cooperation and conflict, with new clashes sparked by every new internal incident or relevant technological advance.

The State Secrets Bureau

One of the hallmarks of single-party authoritarian system are well-developed organizational structures for the protection of information deemed to be "state secrets." The regime in Beijing is no exception, possessing a sophisticated and interlocking set of secrecy-oriented units at all levels of the party. Of these, the most important is the State Secrets Bureau.

The State Secrets Bureau (SSB) is directly responsible for the protection of state secrets by all Chinese government and party organizations. Under the PRC Law on the Protection of State Secrets state secrets are defined as "matters that affect the security and interests of the state," including broad areas of national defense, diplomatic affairs, policy decisions on state affairs, national economic and social development, political parties and "other state secrets that the State Secrets Bureau has determined should be safeguarded."

In reality, however, many seemingly trivial pieces of information in China, such as company revenue numbers, are hidden under the cloak of "state secrets," and information has been known to be retroactively declared a state secret to further the political agenda of an individual, unit, or the state itself.

The State Secrets Bureau has sought to extend its jurisdiction over Internet content. In January 2000, the bureau extended the State Secrets Law to the Internet. The new *"State Secrecy Protection Regulations For Computer Information Systems on The Internet"* explicitly prohibits computer information systems that contain state secrets from being directly or indirectly connected to the Internet or other public information networks. Second, the regulations prohibit the storage, processing, or transmission of state secrets over the Internet. Finally, individuals and units are prohibited from releasing, discussing, or transmitting state secrets on electronic bulletin boards, chat rooms, or Usenet groups. Operators of chat rooms will be held liable for their content. If they find something that is "*obviously wrong*", they must delete it, while if they find content that is suspicious, they should report it. Web site operators must undergo computer security checks, and those that have failed to implement safeguards against security breaches will be shut down. In

addition, Web sites will not be permitted to hire "cyber reporters" to write stories for them, but must get content from China's state-controlled media since site operators may not publish previously unreleased information on the Internet without permission.

Conclusion

Analysts disagree about the impact that this blizzard of new legislation will have. Some say it will have relatively little effect since many Web site operators have long known that leaking state secrets on the Internet is going to be an illegal activity. Provisional regulations to this effect have been circulating since early 1998. Webmasters are already self-censoring, taking their political news from official media sources only, or steering clear of such content altogether and focusing instead on sports and entertainment.

Many believe the new rules to be unenforceable due to the high cost and impracticality of monitering the exploding volume of information being exchanged via the Internet and tracing them to particular individuals. It may be technically possible to filter out keywords and read email, they say, but it will considerably slow down Internet communication and therefore development, to which the economic departments are likely to make strenuous objections. At the same time, many Chinese Web site operators have said that the regulations were inevitable and that in a sense they are useful for standardizing irregular practices and bringing order to the industry. Others however, assert that the regulations concerning cyber-reporting may be a disaster for some Chinese Internet portal sites, which depend on their own news reports and those from other providers for content.

Even where there is little direct impact from the new legislation, it will indirectly repress the atmosphere of lively on-line debate that characterised the early days of the Internet in China. In addition, the new rules are likely to hinder technical innovation, while the constantly shifting interpretations and contradictory implementations may frighten off foreign direct investment, undermining China's efforts to exploit the economic potential of the Internet.

Key Internet Legislation and Regulations issued in China since 1996
(NB: Keep the bold in the layout)

"PRC Interim Regulations Governing the Management of International Computer Networks"
PRC Interim Regulations Governing the Management of International Computer Networks (*Zhonghua renmin gongheguo jisuanji xinxi wangluo guoji lianwang guanli zanxing guiding*),
pub. Fazhi Ribao (*Legal Daily*), February 12, 1996,
issued by State Council Order No.195, signed by Premier Li Peng on February 1, 1996.

"Management Measures of the PRC Regulations for the Safety Protection of Computer Information Systems"
Management Measures of the PRC Regulations for the Safety Protection of Computer Information Systems (*Jisuanji xinxi wangluo guoji lianwang anquan baohu guanli banfa.*),
pub. Jisuanji Ji Wangluo - Falu Fagui (*Computers and Internet -Laws and Regulations*),
Falu Chubanshe, Beijing: 1999, p. 99.

"State Secrecy Protection Regulations For Computer Information Systems on the Internet"
Regulations Regarding Management of State Secrets in Computer Information Systems and International Internet (*Jjisuanji xinxi xitong guoji lianwang baomi guanli guiding*) January 25, 2000 (applied retroactively from January 1, 2000) issued by the Bureau for the Protection of State Secrets.

"PRC Telecommunications Regulations"
PRC Telecommunications Regulations (*Zhonghua renmin gongheguo dianxin tiaoli*),.October 11, 2000,
issued by State Council Order No.291, endorsed by Premier Zhu Rongji on September 25, 2000.

"Telecommunications Regulations Of The People's Republic Of China"
PRC Telecommunications Regulations (*Zhonghua renmin gongheguo dianxin tiaoli*),.October 11, 2000, issued by State Council Order No.291, signed by Premier Zhu Rongji on September 25, 2000.

"Measures for Managing Internet Information Services"
Measures for Managing Internet Information Services (*Hulianwang xinxi fuwu guanli banfa.*), *Fazhi Ribao* (*Legal Daily*),
issued by State Council Order No.292; signed by Premier Zhu Rongji on September 25, 2000.

"Decisions of the National People's Congress Standing Committee on Safeguarding Internet Safety"
Decisions of the National People's Congress Standing Committee on Safeguarding Internet Safety (*Quanguo renda changweihui guanyu weihu hulianwang anquan de guiding*), *Fazhi Ribao (Legal Daily)*, December 30, 2000.

"Explanations on Certain Questions Concerning the Specific Application of Law in the Trial of Cases of Stealing, Making Secret Inquiries of or Buying State Secrets and Intelligence and Illegally Providing Gathered State Secrets and Intelligence for Units Outside the Country",
in "China: Supreme People's Court on Stealing State Secrets", BBC Monitoring, January 23, 2001, from report in Xinhua, January 21, 2001.

THE HACKTIVISMO DECLARATION
assertions of liberty in support of an uncensored internet

DEEPLY ALARMED that state-sponsored censorship of the Internet is rapidly spreading with the assistance of transnational corporations,

TAKING AS A BASIS the principles and purposes enshrined in Article 19 of the Universal Declaration of Human Rights (UDHR) that states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers", and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) that says,

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this Article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order, or of public health or morals.

RECALLING that some member states of the United Nations have signed the ICCPR, or have ratified it in such a way as to prevent their citizens from using it in courts of law,

CONSIDERING that, such member states continue to willfully suppress wide-ranging access to lawfully published information on the Internet, despite the clear language of the ICCPR that freedom of expression exists in all media,

TAKING NOTE that transnational corporations continue to sell information technologies to the world's most repressive regimes knowing full well that they will be used to track and control an already harried citizenry,

TAKING INTO ACCOUNT that the Internet is fast becoming a method of repression rather than an instrument of liberation,

BEARING IN MIND that in some countries it is a crime to demand the right to access lawfully published information, and of other basic human rights,

RECALLING that member states of the United Nations have failed to press the world's most egregious information rights violators to a higher standard,

MINDFUL that denying access to information could lead to spiritual, intellectual, and economic decline, the promotion of xenophobia and destabilization of international order,

CONCERNED that governments and transnationals are colluding to maintain the status quo,

DEEPLY ALARMED that world leaders have failed to address information rights issues directly and without equivocation, RECOGNIZING the importance to fight against human rights abuses with respect to reasonable access to information on the Internet,

THEREFORE WE ARE CONVINCED that the international hacking community has a moral imperative to act, and we DECLARE:

- THAT FULL RESPECT FOR HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS INCLUDES THE LIBERTY OF FAIR AND REASONABLE ACCESS TO INFORMATION,WHETHER BY SHORTWAVE RADIO, AIR MAIL, SIMPLE TELEPHONY, THE GLOBAL INTERNET, OR OTHER MEDIA.

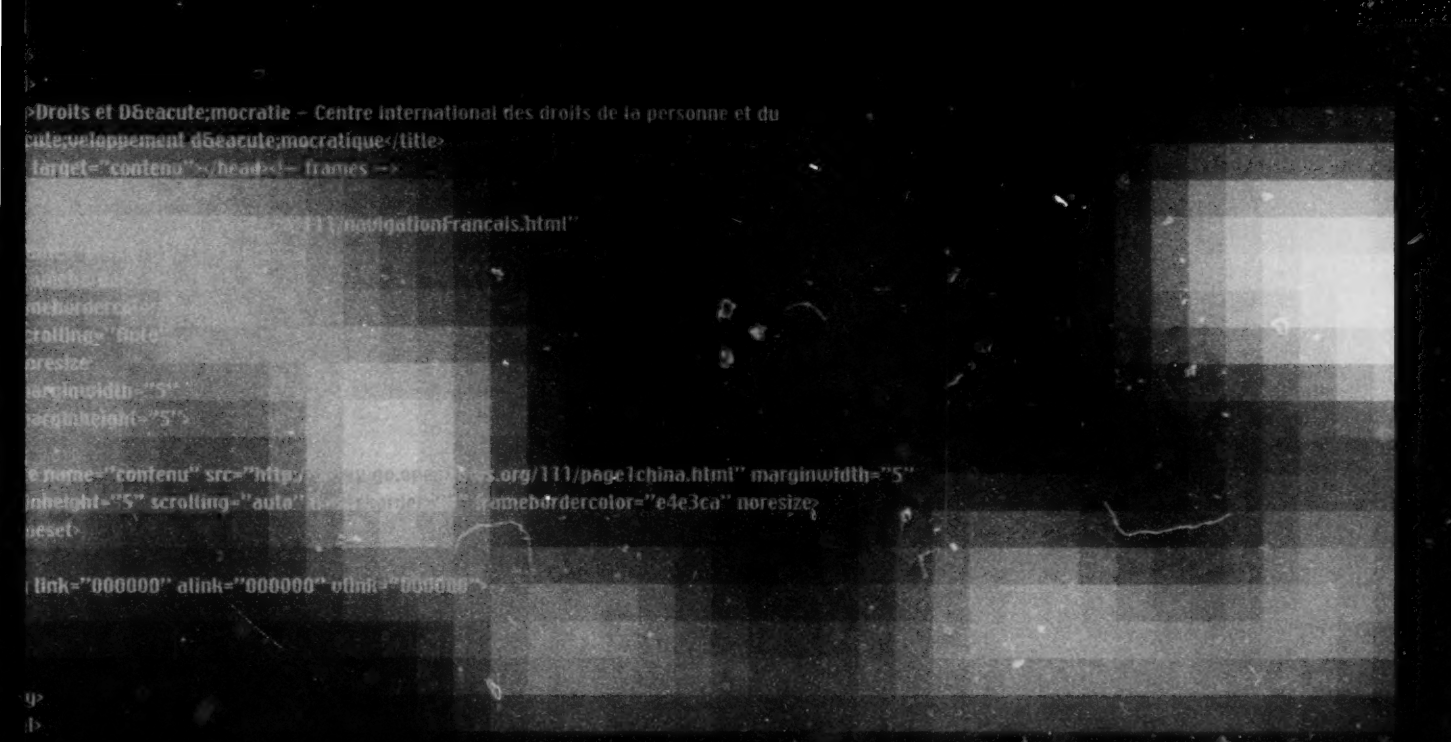
- THAT WE RECOGNIZE THE RIGHT OF GOVERNMENTS TO FORBID THE PUBLICATION OF PROPERLY CATEGORIZED STATE SECRETS, CHILD PORNOGRAPHY, AND MATTERS RELATED TO PERSONAL PRIVACY AND PRIVILEDGE, AMONG OTHER ACCEPTED RESTRICTIONS. BUT WE OPPOSE THE USE OF STATE POWER TO CONTROL ACCESS TO THE WORKS OF CRITICS, INTELLECTUALS, ARTISTS, OR RELIGIOUS FIGURES.

- THAT STATE SPONSORED CENSORSHIP OF THE INTERNET ERODES PEACEFUL AND CIVILIZED COEXISTENCE, AFFECTS THE EXERCISE OF DEMOCRACY, AND ENDANGERS THE SOCIOECONOMIC DEVELOPMENT OF NATIONS.

- THAT STATE-SPONSORED CENSORSHIP OF THE INTERNET IS A SERIOUS FORM OF ORGANIZED AND SYSTEMATIC VIOLENCE AGAINST CITIZENS, IS INTENDED TO GENERATE CONFUSION AND XENOPHOPIA, AND IS A REPREHENSIBLE VIOLATION OF TRUST.

- THAT WE WILL STUDY WAYS AND MEANS OF CIRCUMVENTING STATE SPONSORED CENSORSHIP OF THE INTERNET AND WILL IMPLEMENT TECHNOLOGIES TO CHALLENGE INFORMATION RIGHTS VIOLATIONS.

Issued July 4, 2001 by Hacktivismo and the CULT OF THE DEAD COW.

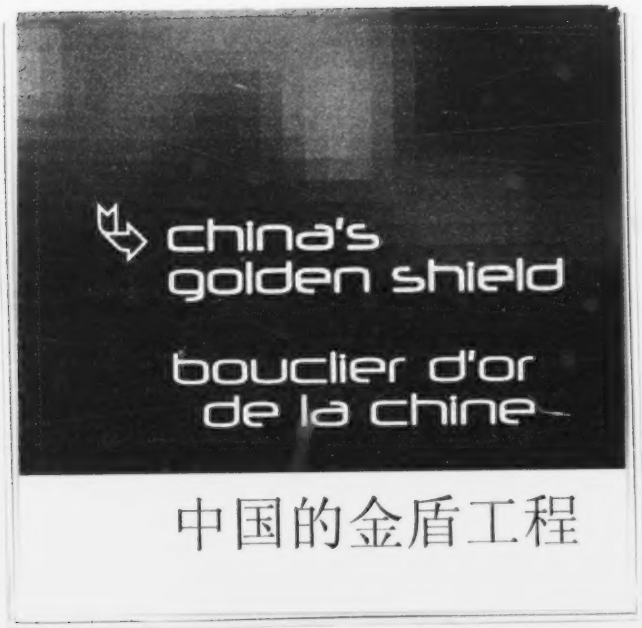


china's golden shield

Corporations and the Development of Surveillance Technology in the People's Republic of China

enter

by
Greg Walton


china's
golden shield
bouclier d'or
de la chine
中国的金盾工程

Rights & Democracy is a Canadian institution with an international mandate. It works with civil society and governments in Canada and abroad to promote human rights and democratic development through dialogue, advocacy, capacity building and public education. It focuses on four themes: democratic development, women's rights, rights of indigenous peoples, and globalization and human rights; as well as two special operations: International Human Rights Advocacy and Urgent Action/Important Opportunities.

Author:
Greg Walton is a freelance researcher focusing on the impact of technology and globalization on human rights and democracy. He is currently developing disruptive compliance strategies for a range of transnational, non-profit organizations. His homepage is go.openflows.org/jamyang.

Acknowledgements:
Carole Samdup, Diana Bronson, and all at Team R&D. OxBlood Ruffin, cDc, Drunken Master and the Hacktivismo! Project. y Oda, the Google cache, Kundrel core, SafeWeb, Dr. Patrick Ball, Jenny 8, Wyrds of Simple Nomad, Openflows, M&D, and so many others – on both sides of the firewall – who very sensibly choose to remain anonymous. For now ;-)

© International Centre for Human Rights and Democratic Development, 2001.

This publication is available free of charge and may be freely excerpted, provided credit is given and a copy of the publication in which the material appears is sent to Rights & Democracy.

Legal Deposit: Bibliothèque nationale du Québec, fourth quarter 2001.
National Library of Canada, fourth quarter 2001. ISBN: 2-922084-42-6.

Graphics: Laperrière Communication
Printed in Canada.

China's Golden Shield 1.0 is available at www.ichrdd.ca.
It is also published as an Open Source Human Rights Report at: go.openflows.org.

FREEDOM_OF_SPEECH : FREEDOM_OF_CODE

China's Golden Shield

Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.

The Universal Declaration of Human Rights, Article 28

"... it's a little strange to tie free trade to human rights issues, it is basically getting down to interference in internal affairs."[1]

Bill Gates, then CEO of Microsoft,
standing shoulder to shoulder with Jiang Zemin during a photo-op in Beijing, 1994.

103-02095/

Table of Contents

Preface 04
Executive Summary 05
Introduction 08
Box 1: Paying the Price for Freedom 10

Technology Transfer and Policy Convergence 11
Operation Root Canal 12

What do You Want the Internet to Be?
"A human touch. I want it to know who I am." 14
China's Golden Shield 15
Box 2: China's Golden Projects: Modernizing the Chinese Economy 17
Unholy Alliance 17
Beyond the Great Firewall 18
Making the Internet Personal 20
The Subscriber Edge 23
A Virtual Shadow 24
A Network that Knows Who and Where You Are 25
Box 3: "Neutral" Technology at Tiananmen Square 26
Diagram 1: A New Model for the Internet: Innovation at the Edge of the Network 27
Diagram 2: Interaction Across a Firewall 27

Conclusion – "The mouse is mightier than the missile" 28
Appendix: How to Use the CD-ROM that Accompanies this Report 29
Liner Notes 29

Glossary 32

Endnotes 36

Preface

Information and communication technology is often described as the driving force behind globalization. It is also promoted as a tool for democratization with connectivity heralded as the end of the digital divide. In truth, there is no doubt that electronic communication has facilitated the flow of information around the globe and that it has increased opportunities for human rights and democracy activists to build international support for their struggles.

Unfortunately, the advent of modern communication technology has also brought new challenges for human rights advocates, particularly those living under repressive regimes. In a world where the rules of international trade are unconnected to international human rights law, technology's promise of democratization is threatened by economic priorities. In the People's Republic of China, where there is no democratic accountability or legislative protection of human rights, technology can be and has been used as an instrument of repression.

At stake is the right of all people to an international order within which the promise of the Universal Declaration of Human Rights (UDHR) can be fulfilled. The UDHR and its accompanying covenant on civil and political rights protect fundamental human rights including the individual's right to privacy. The protection of human rights is the obligation of governments and must be reflected in all activities implemented under governmental authority whether they are trade promotion activities, the negotiation of bilateral and international trade agreements, export financing or development assistance.

This report reveals how sophisticated technology, developed in Canada and promoted through a series of national and international processes, could undermine the principles enshrined in human rights agreements. China's Golden Shield project threatens the protection of human rights, in particular the right to privacy – a right that underpins other essential elements of democracy activism such as freedom of association and freedom of expression. It positions the alliance of government and business in opposition to those standing on the cyber-frontline of the human rights movement in China today.

It is my hope that this paper will provide a glimpse into the world of high-tech, big business and the struggle for human rights and democracy in China. On behalf of Rights & Democracy, I offer it in the spirit of solidarity with the people of China who may find its content of some use as they develop and consolidate social movements for change. I offer it also to my fellow Canadians who, following recent reports on police surveillance of dissent in Canada, may discover how intimately the rights of citizens in China are linked to our own.

Warren Allmand, P.C., O.C., Q.C.

President

Executive Summary

China today faces a very modern paradox. On one side, the government understands that information technologies are the engine driving the global economy, and that Chinese economic growth will depend in large measure on the extent to which the country is integrated with the global information infrastructure. At the same time, however, China is an authoritarian, single-party state. Continued social stability relies on the suppression of anti-government activities. To state the problem simply, political control is dependent on economic growth and economic growth requires the modernization of information technologies, which in turn, have the potential to undermine political control.

The "Great Firewall of China" is failing, largely due to the increased volume of Internet traffic in China. The government knows that it can no longer hope to filter out all "objectionable" material before it enters China's networks; and so, faced with these contradictory forces of openness and control, China is seeking to strike a balance between the information-related needs of economic modernization and the security requirements of internal stability. In seeking to reach this balance, the Chinese state has found an extraordinary ally in private telecommunications firms located primarily in Western countries. Many companies, including notably Nortel Networks, until recently Canada's largest firm, are playing key roles in meeting the security needs of the Chinese government. Nortel Networks and other international firms are in effect helping China to displace the firewall it constructed at the international gateway with a more sophisticated system of content filtration at the individual level.

Old style censorship is being replaced with a massive, ubiquitous architecture of surveillance: the Golden Shield. Ultimately the aim is to integrate a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies. This has been facilitated by the standardization of telecommunications equipment to facilitate electronic surveillance, an ambitious project led by the Federal Bureau of Investigation (FBI) in the US, and now adopted as an international standard.

Many people in China have been arrested for Internet-related "crimes," ranging from supplying e-mail addresses to Internet publications to circulating pro-democratic information or articles that are critical of the Chinese government, in blatant contradiction of international human rights law guaranteeing freedom of speech. Charges are typically "subversion" or "threatening to overthrow the government" as the line between criminal activity and the exercise of freedom of speech is non-existent in China. The development of this new all-encompassing architecture of electronic surveillance will make the lives of such courageous activists even more difficult.

In November 2000, 300 companies from over 16 countries attended a trade show in Beijing called Security China 2000. Among the organizers was the "Chinese Communist Party Central Committee Commission for the Comprehensive Management of Social Security." A central feature of the show was the Golden Shield project, launched to promote "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work." China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to records on every citizen in China, while linking to vast networks of cameras designed to increase police efficiency.

In order to make the Golden Shield a reality, the Chinese government is dependent upon the technological expertise and investment of Western companies. Canada's Nortel Networks is playing a key role in these developments as witnessed by:

> its joint research with Tsinghua University on specific forms of speech recognition technology, for the purpose of automated surveillance of telephone conversations;

> its strong and early support for FBI plans to develop a common standard to intercept telephone communications, known as CALEA, in conjunction with technology transfer through its joint venture, Guangdong Nortel (GDNT);

> its close relationship with Datang Telecom, a Chinese firm with substantial interests in the state security market in China;

> the promotion of JungleMUX which allows video surveillance data to be transported from remote cameras back to a centralized surveillance point to the Chinese Ministry of Public Security (MPS);

> the deployment of its "Personal Internet" suite in Shanghai, greatly enhancing the ability of Internet service providers to track the communications of individual users;

> a US$10 million project to build a citywide fibre-optic broadband network in Shanghai (OPTera) enabling central authorities to monitor the interests of subscribers at the "edge" of the network, principally through the Shasta 5000 firewall, in direct conflict with the right to privacy. This technology will also make it more difficult for dissidents to have clandestine communications and facilitate police monitoring of Internet users attempting to access URLs not judged appropriate by the Chinese government;

> the integration of face recognition and voice recognition technology in collaboration with AcSys Biometrics, a subsidiary of Burlington, Ontario-based NEXUS.[2]

Many other Western firms have been involved in the development of a repressive state security apparatus through the following developments:

> a nationwide database containing information on all adult Chinese citizens;

> smart cards for all citizens which can be scanned without the owner's knowledge at a distance of a few metres;

> closed-circuit television to monitor public spaces;

> technology which allows the Public Security Bureau to make instant comparisons of fingerprints;

> development of firewalls in China.

The self-interested high-tech discourse promises that new information and telecommunication technologies are inherently democratic and will foster openness wherever they are used. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China* debunks this myth. Technology is embedded in a social context and, in this report, it has been shown to bolster repression in a one-party state in the name of expanding markets and exponential profits.

Introduction

China has long suffered from inadequate telecommunications. Economic growth has demanded modernization of an infrastructure characterized by outdated technology and limited access to the resources necessary to develop it. To overcome these deficits, the government has embarked on a well-financed effort to modernize its information infrastructure. China has therefore quickly become one of the world's largest consumers of telecommunications equipment.

An important goal of this modernization has been the acquisition of advanced telecommunications equipment from industrialized nations, on the premise that the technologies of the information revolution provide China with the opportunity to "leapfrog" and vastly improve capabilities in areas related to telecommunications. The transfer of these technologies to China has been facilitated by two mutually supporting trends.

First, there is enormous competition among telecommunications firms to get a share of the relatively undeveloped but rapidly expanding Chinese telecommunications market – the largest market in the world. Naturally, the lure of potential billions has attracted every major telecommunications corporation, including US-based Lucent and Cisco, European wireless giants Nokia and Ericsson, and Canada's Nortel Networks – not to mention countless others. From these companies, China is buying more than US$20 billion worth of telecom equipment a year.

China is reported to account for about 25% of the world's market for telecommunications equipment and is expanding exponentially. Much of this growth is achieved through sales by foreign telecommunications companies and by joint ventures with Chinese partners, which brings us to the second important trend.

The installation of an advanced telecommunications infrastructure to facilitate economic reform greatly complicates the state's internal security goals. As the amount of information traveling over China's networks increases exponentially, the government's ability to control that information declines.

The exponential growth of the Internet in China has led some to argue that as new technologies are adopted they will inevitably create a more open, democratic society. The premise of much research is that the Internet is an inherently democratizing medium, promoting pluralism, strengthening civil society, and pressuring governments to become more accountable to their people. In the post-Cold War world, the power of information and communication technology to transform repressive societies is often held to be self-evident.

Recent events in China present a rather different story. It is well documented that the Chinese government is committed to controlling online content and to restricting the access citizens have to information published outside the country.[3] They also aim to prevent the emergence of "virtual organizing" that has become an important feature of the Internet in other countries. In this regard, the Internet presents a number of unique challenges to the regime. Recent data from a Chinese Academy of Social Sciences (CASS) survey shows that 10% of users admit to regularly using proxy servers to defeat censorship, that most users trust foreign news

sources almost as much as government sources, and that the majority believe that the Internet will have significant social and political effects.[4]

In light of this rapid transformation, Chinese authorities are keen to acquire new technologies that will serve to increase their surveillance capabilities. While the Internet may empower ordinary people, it may also provide the government with a new range of repressive tools to monitor private speech and censor public opinion.

Chinese President Jiang Zemin, left, shakes hands with Frank Carlucci, chairman of Nortel Networks of Canada, in March 2000 in Beijing

From the first linking of China to the global internet in 1994, central authorities have consistently sought to control China's Internet connections. Heavily restricting international connectivity was a key principle in China's nascent Internet security strategy. Now, seven years later, international connections for all five of China's major networks[5] still pass through proxy servers at official international "gateways."[6] Filtering and monitoring of network traffic is still focused at this level. Derisively termed "The Great Firewall"[7] by hackers and journalists worldwide, this strategy has enjoyed varying degrees of success. Continued economic modernization, however, has led to exponential growth in the demand for international bandwidth, and the sheer volume of Internet traffic today poses a serious challenge to the strategy of State control at the gateway level.

Originally, there were many reasons for constructing the Chinese network along the lines of this "Great Firewall" model. The gateways would modulate the pace of China's opening up to the world through electronic interaction. The government would decide at what rate to expand the connections and could theoretically shut them down in a social emergency.

The gateways were to serve as the first line of defence against anti-government network intrusions. They would serve as a firewall, restricting the amount of information about internal networks available to foreign intruders. The gateways were designed to prevent Chinese citizens from using the Internet to access forbidden sites and anti-government information from abroad. In theory, State control of the routing tables at the gateway level offered authorities the hope that they could prevent their own people from accessing foreign sites like the Cable News Network (CNN), the British Broadcasting Corporation (BBC), the Tibet Information Network or Human Rights Watch/Asia.

China's Internet regulations and legislation are guided by the principle of "guarded openness" – seeking to preserve the economic benefits of openness to global information, while guarding against foreign economic domination and the use of the Internet by domestic or foreign groups to coordinate anti-regime activity.

The stakes are high – for the government, as China integrates into the global economy, and for the would-be "cyber-dissident," who ultimately faces the death penalty for illegal use of the Internet.

Box 1:

Paying the Price for Freedom

In January 2001, the official news agency Xinhua announced that anyone involved in "espionage activities" such as "stealing, uncovering, purchasing or disclosing State secrets" using the Web or by other means risks the death penalty, or 10 years to life in prison.

> On January 18, 2000, the dissident Leng Wanbao was interrogated for three hours after circulating a letter from another dissident to people outside China over the Internet. The police reminded Leng Wanbao that sending such a letter was against the country's public security laws.

Lin Hai, a computer entrepreneur, was charged with subversion in 1998 for supplying Chinese e-mail addresses to a pro-democracy Internet magazine.

> On March 3, 2000, Lin Hai, a software entrepeneur, who had been condemned to two years in prison for "inciting others to overthrow the State," was freed from prison. Arrested in 1998, he had been convicted of supplying 30,000 Chinese e-mail addresses to overseas dissident publications, notably *VIP Reference*. These publications had used the addresses to distribute dissenting articles over the Internet. Freed in the greatest secrecy in September 1999, Lin Hai was very hesitant to speak of his situation, suggesting that the authorities had offered him early release in exchange for his silence. At his release, Lin Hai called himself "the first Chinese Internet prisoner."

> On June 3, 2000, Huang Qi, manager of www.6-4tianwang.com, which contains a discussion forum, was arrested and accused of "subversion." The authorities accused him of publishing articles on his Web site, which is hosted in the US, condemning the Tiananmen massacre in June 1989. It contained an open letter from the mother of a young student killed during the massacre, calling for the renewal of the 1989 pro-democratic movement. Huang Qi's computer and all of the documents found in his office and home were confiscated. The site, open to "all those who have something to say," is still updated by Chinese dissidents who live in the US, but mainland Internet users can no longer access it.

> On August 16, 2000, the police interrogated Jiang Shihua, a professor of computer science in the Sichuan province in south-western China. He was accused of "inciting subversion." He used the cybercafé that he owned, the Silicon Valley Internet Coffee, in Nanchong, to circulate articles criticizing the authorities, and published pro-democracy articles in an Internet newsgroup. He has been charged with "inciting others to overthrow the State." This case has still not gone to trial.

> Qi Yanchen, editor of the online publication *Consultations*, was convicted on September 19, 2000, to four years in prison for "subversion" and "circulation of anti-governmental information over the Internet." The MPS claims that he used the pseudonym Ji Li to write articles for the Hong Kong monthly *Kaifang* and the dissident newsletter *VIP Reference*. He also published excerpts of his book, *The Fall of China*, advocating political reform. The police confiscated his computer, his fax and his notes.

> On May 13, 2000, the government suspended the China Finance Information Network site for two weeks and ordered its owners to pay a fine. The online financial publication was accused of having circulated rumours that could damage the image of the government. This conviction followed the publication of an article on corruption concerning a local political official.

> On August 3, 2000, security officials disconnected and banned www.xinwenming.net for having circulated "counter-revolutionary information" and attracting a "large part of the Chinese dissident community." The five dissidents behind the site are currently wanted by the police, but have not yet been arrested. Created April 29, 2000, www.xinwenming.net is the first site hosted in China to openly call for "national reconciliation and democracy."

Technology Transfer and Policy Convergence

The Right to Freedom of Opinion, Expression and Information

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The Universal Declaration of Human Rights, Article 19

Globalization erodes national control of the flow of data. The development of the Internet is perhaps the best known example of a global technology. The combination of globalization and digital convergence is having a devastating effect on privacy in many developing countries. In the field of information and communication technology, the speed of policy convergence is accelerating to such an extent that even the most developed nations can hardly keep up with advances in technology. Across the digital surveillance spectrum – wiretapping, personal ID systems, data mining, censorship or encryption controls – it is the industrialized countries that invariably set the rules for the rest of the world.

There is increasing concern that much of this surveillance technology is being exported, without any end-use criteria, to countries that flagrantly abuse the fundamental human rights of their citizens. Governments of countries with poorly developed infrastructures rely on industrialized countries to supply them with surveillance equipment. The transfer of surveillance technology from the developed to the developing world is now an important component of the post-Cold War arms industry.[8] With scant attention given to differing levels of human rights compliance, standardization across national borders is leading many to argue that a global architecture of electronic surveillance is emerging, with its origins in the US law enforcement community.

Operation Root Canal

As early as 1988, in a program known internally to the US Federal Bureau of Investigation (FBI) as "Operation Root Canal,"[9] US law enforcement officials demanded that telephone companies alter their equipment to facilitate the interception of messages. All but one of the major global telecom companies refused to contemplate altering their equipment. The exception was a Canadian company, Nortel Networks, which agreed to work closely with the FBI.[10] More than 75% of North American Internet backbone traffic travels across Nortel Networks systems, and the company derives a significant proportion of its sales revenue from the US telecom market.

After several years of lobbying by the FBI, the US Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[11] CALEA requires that terrestrial carriers, cellular phone services and other telecom equipment manufacturers ensure that all their "equipment, facilities or services" are capable of "expeditiously... enabling the government... to intercept... all wire and oral communications carried by the carrier... concurrently with their transmission."[12] Communications must be in such a form that they can be transmitted to a remote government facility.

CALEA redefines the telecommunications industry's obligation to assist law enforcement in executing lawfully authorized electronic surveillance. The law directs the telecommunications industry to actively develop solutions to address law enforcement's surveillance requirements. To facilitate compliance, CALEA authorized US$500 million to be appropriated for the purpose of reimbursing the telecommunications industry for certain costs.[13] Manufacturers must work with industry and law enforcement officials to ensure that their equipment meets federal standards. A court can fine a company US$10,000 per day for each product that does not comply.[14]

The passage of CALEA was controversial, not least because the FBI continuously sought to include more and more rigorous regulations under the law. These included requirements that cellular phones allow for location-tracking on demand and that telephone companies provide capacity for up to 50,000 simultaneous wiretaps.[15]

While the FBI lobbied Congress and pressured US companies into accepting CALEA, it also pressured US allies to adopt it as an international standard. The FBI began working with the Justice and Interior Ministers of the European Union (EU) towards creating international technical standards for wiretapping.[16] In 1991, the FBI held a series of secret meetings with EU member states to persuade them to incorporate CALEA into European law. In 1993, the FBI began hosting meetings at its research facility in Quantico, Virginia called "International Law Enforcement Telecommunications Seminars" (ILETS). The meetings included representatives from Canada, Hong Kong, Australia and the EU. At these meetings, an international technical standard for surveillance, based on the FBI's CALEA demands, was adopted as the "International Requirements for Interception."[17]

The plan, according to an EU report,[18] was to call for the industrialized world to agree to norms and procedures and then sell their products to developing countries. Even if they did not agree to interception orders, they would find their telecommunications monitored by the UK-USA signals intelligence network "the minute they used the equipment."[19] The FBI's efforts resulted in an EU Council of Ministers resolution that was quietly adopted in January 1995. The resolution's text was almost word for word identical to the FBI's domestic requirements.[20] The resolution was not formally debated, and was not made public until late 1996.

The ILETS group continued to meet. A number of committees were formed and developed a more detailed standard, which extended the scope of the interception standards. The new standards were designed to apply to a wide range of communication technologies, including the Internet and satellite communications. It also set more detailed criteria for surveillance across all technologies. The result was a 42-page document called ENFOPOL 98 (the EU designation for documents created by the EU Police Cooperation Working Group).[21] In 1998, the document entered the public domain and generated considerable criticism. The committees responded by removing most of the controversial details and producing a new document, called ENFOPOL 19, expanding the type of surveillance to include "IP address, credit card number and e-mail address."[22] In April 1999, the Council proposed the new draft council resolution to adopt the ENFOPOL 19 standards into law in the EU.

In May 1999, the European Parliament approved the ENFOPOL 19 resolution. The vote was taken late on a Friday evening with only 20% of the delegates present, and was subsequently reversed by the Council of Ministers. The rejection has not stopped the European Telecommunications Standards Institute (ETSI) from continuing its work on developing international wiretapping standards.

What do You Want the Internet to Be?

"A human touch. I want it to know who I am."[23]

At a trade show held in Beijing in November 2000, the biggest names in Web technology – "companies that proudly attach themselves overseas to the Internet's reputation for anarchy"[24] – peddled their wares to China's secret police and security officials. Billed as the "largest national security exhibition," Security China 2000 was the second such event sponsored by the Ministry of Public Security (MPS) in as many years. Among the organizers listed was the "Chinese Communist Party Central Committee's Commission for the Comprehensive Management of Social Security,"[25] a body which is in overall charge of the state security apparatus, from controls over migrant workers, to anti-crime campaigns and monitoring dissident activity.

Shanghai Business Magazine recently estimated that the Chinese security industry is enjoying 15% annual growth. Overseas specialists cited in the trade journal *Security World* predict 20% growth for the next three to five years. China is expected to become the second largest security market after the US within 10 years.[26]

The trade show was organized by Hong Kong-based Adsale Exhibition Services Ltd. and drew approximately 300 companies from over 16 countries, as well as 24,500 visitors from over 26 of China's provinces. Special guests included Jia Chunwang, Minister of Public Security. According to Adsale, in comparison to the first Security China exhibit in 1998, in 2000 "the show boasts a 50% increase in international exhibitors and an 80% growth in exhibit space area."[27] Exhibitors included network giants Siemens, Motorola, Cisco Systems, Sun Microsystems, and Nortel Networks. There were participating companies from the US, Israel, France, Germany, the Netherlands, Japan, and Canada, among others. The United Kingdom, world leader in closed-circuit TV, had a special section in the show.

The focus of Security China 2000 quickly became the MPS' new Golden Shield project, launched to promote "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work."[28] China's security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance. Beijing envisions the Golden Shield as a database-driven remote surveillance system – offering immediate access to registration records on every citizen in China, while linking to vast networks of cameras designed to cut police reaction time to demonstrations.

Though the project is still in its infancy, Chinese industry executives at the trade fair estimated that the government had spent RMB 600 million (US$70 million) on research to date, and that the total spending would likely run many times that.

The Golden Shield project, according to information on the conference Web site, is focused on the following fields of security: "Access Control, Anti-Hacker Intrusion, Communication Security, Computer Accessories & Software, Decryption & Encryption, E-commerce Security, Extranet & Intranet Security, Firewalls, Networking Communications, Network Security & Management, Operation Safety, Smartcard Security, System Security, Virus Detection, IT-related Services and Others."[29]

The success of the Golden Shield project depends on a wide range of advanced technologies. While Chinese research is advancing rapidly in these areas, and other related fields, Chinese scientists have developed none of the components necessary to implement Golden Shield independently. In each case, they have relied on assistance from Western corporations, either by purchasing components as turnkey solutions, or through technology transfer – either through formal business deals or in exchange for greater market access.

The technologies necessary to support an intelligent mass surveillance network are frighteningly complex. However, since the solutions are modeled on human forms of intelligence we can categorize them in terms familiar to everyone: Beijing's Golden Shield surveillance network is intended to be able to "see," to "hear," and to "think."

The technology behind the network's ability to "hear" – to automatically monitor telephone conversations, searching for key words and phrases, for example – centers on speech signal processing. Similarly, video signal processing lies behind a surveillance camera's ability to "see," that is, to recognize individual faces in a crowd of people. Both "senses," forms of digital signal processing (DSP), are termed "algorithmic surveillance" systems, which is data analysis via complex algorithms modeled on the human nervous system. In speech signal processing, for example, the cochlea might be the basis for mathematical abstraction.

In China the leader in each of these fields is the Department of Electronic Engineering at the prestigious Tsinghua University. A research group there has been working on speech recognition since the early 1980s. This research is financially supported by both the Chinese government and Nortel Networks (from 1995 to 1998).[30] It parallels Nortel's own speech recognition research in association with the FBI.

The funds from the Chinese government for the speech recognition project come out of the National 863 High Technology Projects Budgets.[31] The 863 Project was initiated in March 1986 as China's response to the Reagan Administration's Strategic Defense Initiative/"Star Wars."[32] The 863 concentrates government investment in seven distinct areas, including information technology, which have military and state security applications. Other examples of 863 investments include lasers and anti-satellite systems, and some 863 projects are supervised by the Chinese Weapons Development Agency.[33]

By the end of 1998, Tsinghua's engineers announced that they were developing a "large vocabulary speaker independent continuous commands recognition system over telephone channel. This real-time system is used for telephone exchange machine and information service system over telephone connections with the recognition rate over 98%."[34] Future research, they added, will focus on "large vocabulary (if not unlimited) speaker-independent continuous speech recognition, and large vocabulary telephone-based speech recognition... to develop a fast speaker adaptive technology, which can efficiently improve the accuracy of the speaker independent recognition."[35] Such a system parallels the development of the technology required to implement CALEA in the US; in other words it would appear to have no other purpose apart from automated surveillance of telephone communications.

Box 2:

China's Golden Projects:

Modernizing the Chinese Economy

The **Golden Projects** were China's telecommunication and information infrastructure initiatives in the 1990s. The projects were categorized into four phases:

Phase One was comprised of four projects: **Golden Bridge** – the infrastructure for the China National Economic Information Network; **Golden Gate** (Customs) – a foreign trade information network linking the Ministry of Foreign Trade and Economic Cooperation with the Customs Bureau; **Golden Card** – an experimental electronic money project; and **Golden Sea** – an information system linking China's top government leaders and providing them with live access to data from all the institutions, organizations, and offices under the direct jurisdiction of the Communist Party Central Committee.

The projects in Phase Two were designed to apply information networks to economic reform. They comprised: **Golden Macro** – which was the Government's Central Economic and Financial Leading Group for macro-control over national economic activities; **Golden Tax** – a data network designed to link State Tax Administration's auditing centre in Beijing with 50 regional offices and 800 bureaus; and **Golden Intelligence** China's Internet service.

Projects in Phase Three had to do with sectoral applications of the new IT program. They included **Golden Enterprise** – the construction of intranets in China's 12,000 large and medium-sized enterprises, and their interconnection according to different circles of business; **Golden Agriculture** – a databank service network providing agricultural information, weather reports, and market information; **Golden Health** – the Ministry of Public Health's information exchange system for hospitals; **Golden Information** – a network linking the various statistical collection departments across the country; and **Golden Housing** – a nationwide database of information on real estate. Phase Four of projects included **Golden Cellular** – a consortium of China's largest domestic mobile communications manufacturers; and **Golden Switch** – a program to build China's domestic digital switch manufacturing industry.

Unholy Alliance

Tsinghua's engineering faculty has close ties with the Bell-Northern Research Lab (BNR) in Montreal, a Nortel research and development subsidiary,[36] and the laboratory where Nortel's own speech recognition module (STM) was developed. During the Canadian trade mission to China in 1998, Canadian Prime Minister Jean Chrétien announced that Nortel Networks and Tsinghua would establish a joint research laboratory.[37] A primary goal of the research laboratory was to accelerate the development of networking expertise in China. The agreement also included an "expert exchange program" between Nortel Networks and Tsinghua University to facilitate closer collaboration. Indeed, graduates of Tsinghua's engineering department went on to play key roles in developing Nortel's speech recognition module.

Similarly, Tsinghua has "made statistics of the common sentential forms used for telephone calls. Two hundred and fourteen sentential forms of different commands were collected" to develop the world's largest Chinese speech database.[38]

Given Nortel's early involvement in the development of standards in support of the CALEA legislation, it is natural that the first digital switch to reach market, and give service providers and vendors the ability to meet basic CALEA compliance, should be manufactured by Nortel.[39]

The sophisticated DMS Supernode switching technology is manufactured in China through a joint venture with the Chinese government known as GDNT (Guangdong Nortel). At the time, Nortel said of this technology transfer that it "will contribute immeasurably to the development of the Chinese telecommunications industry."[40]

In terms of funding, Nortel invested an extra US$37 million in GDNT (on top of funds agreed in a 1993 Memorandum of Understanding (MOU) with the state planning commission) – an investment that followed hot-on-the-heels of the announcement that the US government would pay equipment manufacturers compensation for the implementation of CALEA.[41]

Beyond the Great Firewall:

from censorship to surveillance

The pace and scale of the development of China's Internet have reduced the significance of the "Great Firewall" strategy of gateways linking to a secure national "intranet." The original China-wide intranet idea was essentially overtaken by events, in particular the liberalization of the Chinese telecommunications sector.

Despite the official policy of openness suggested by China's pending entry into the World Trade Organization, some officials still cling to the dream of a China-only information network sealed off from the dangerous temptations of the World Wide Web.

"China must build a national network that is independent of the Internet," said Jiang Zemin's son, Dr. Jiang Mianheng, a tech-savvy vice president of the Chinese Academy of Sciences, at a conference in Shanghai last June.[42]

The gateway concept, by contrast, has certainly survived, but has been undermined in part by financial and technical factors. The number and speed of the connections have grown to meet increasingly high business and consumer demand, increasing from 84.64 Mbps in the summer of 1998 to more than 351 Mbps at the end of 1999, and to more than 2.5 Gbps by 2001. Concerns for security and control have partially surrendered to economic demands for broadband convergence networks.

The implications of the construction of firewalls to prevent Chinese people from accessing forbidden materials on sites outside the country are well known. Many of the technologies used in these areas of computer security, however, could also be employed to restrict human rights and democracy through intimidation and systematic surveillance of the population.

The MPS announced last year that within three years it would have created a nationwide computerized database containing personal details and ID numbers for every adult in the country. In the past the Chinese government has kept a cumulative file (called the *dangan*) on every individual's performance and attitudes from kindergarten, and throughout adult employment. This information will now be digitized and Chinese citizens will be issued new, second-generation identification cards that will contain their *dangan* on an embedded microchip. Currently, Chinese ID cards consist of a laminated paper card featuring a person's name, photo, birthday and ID number. This paper card "is relatively easy to counterfeit," said Qiu Xuexin, Director of the No. 1 Research Institute under the MPS,[43] speaking recently at the Fourth International Fair of Smart Cards. Qiu added that by using sophisticated encryption it will be more difficult for unauthorized people to access government information in the new card. The second generation smart card is likely to be a "proximity card" – in other words it can be scanned instantly, from several feet away, without the subject necessarily being aware that he or she is being identified.[44]

In addition, last May, the MPS installed on Chinese Internet service providers two "black boxes" – monitoring devices dedicated to tracking the content and activity of individual e-mail accounts. Furthermore, authorities are working with technology experts at Shenzhen University to develop an "e-mail filtration system" that is able to detect and delete "unwanted" e-mails without the recipient's knowledge or consent.[45] Most recently, the MPS has been involved in creating fake proxy servers to conduct surveillance of surfers who try to circumvent official firewalls.[46]

As in 1998, Security China 2000 was held concurrently with its sister event, Building China 2000. The Golden Shield strategy includes plans to construct "intelligent buildings" and a number of vendors promoted their systems at both trade shows. Following the trade shows Chinese-owned Datang Telecom, recently implicated in an industrial espionage case against Lucent, announced that it had won a contract to construct an intelligent building for the Jilin Provincial Public Security Bureau (PSB):

"Under the contract, Datang Telecom will be responsible for the overall design and implementation of this project, accomplishing all tasks including the construction of security monitoring system, integrated wiring, and computer networking. The implementation of this project attaches demonstrative and promotive significance to the Golden Shield that will be started soon in the national public security sector."[47]

Similar plans to integrate CCTV surveillance networks into the urban environment were recently announced by the MPS in Guangdong on a Web site dedicated to promoting the Golden Shield project.[48]

Datang has also developed its own e-mail filtration package and a number of firewalls. Datang enjoys a number of close relationships with overseas telecom manufacturers, including joint research and technology transfer projects. For instance, Datang has benefited from joint research with Nortel when the two collaborated on a project on CDMA wireless protocol, from which Datang developed a Chinese version of the protocol: TD-SCDMA.

While there is considerable evidence that China is conducting its own advanced research and developing homegrown security systems, the IT security field in China remains essentially

dependent on the expertise provided by transnational corporations, through joint venture partnerships, technology transfers, and direct investment – even at the most basic technological level.

Understandably, corporations are not always keen to publicize such a relationship. Motorola, for example, supplies China's traffic police with wireless communication devices. Journalists reported that company representatives at Security China 2000 "refused to answer questions about the firm's involvement in the Golden Shield project..." Orin Li of Compaq China was equally evasive, claiming: "We are not the only company; everybody's doing it. Go and ask Sun!"[49]

Sun Microsystems is indeed involved in transferring high-tech expertise to the Chinese security apparatus. Working with Changchun's Hongda Group, market leaders in fingerprint recognition technology, Sun Microsystems developed a computer network linking all 33 provincial level police bureaus, forming one layer of the Golden Shield, allowing the PSB instant comparison of fingerprints with a nationwide database.

Cisco Systems is another example, having provided a large proportion of the routers and firewalls in China's network. At Security China 2000 a saleswoman for the computer-network giant Cisco Systems told the group of PSB officials that her company was the world leader in firewalls, and that "China is a large potential market for this kind of technology."[50]

Making the Internet Personal

Right to Privacy

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The Universal Declaration of Human Rights, Article 12

One approach to the problem China's security apparatus faces with the decline in effectiveness of the "Great Firewall" is to shift the focus of content-filtration firewalls from the national level to individual homes and offices – in effect, redistributing the "Great Firewall" from five international gateways to millions of household PCs and cellular phones.

This strategy has profound implications in terms of user privacy – since it makes government surveillance of an individual's traffic a reality, and incorporates technologies that impact heavily on Chinese Internet users right to free expression, making it much more difficult for human rights and democracy activists to communicate with "illegal" information sources, and remain undetected by their government.

This trend, a shift from generalized content control at the gateway level to individual surveillance of users at the edge of the network, is underlined by the advent of new technologies for managing broadband content delivery.

At the Security China 2000 conference Nortel Networks was promoting the JungleMUX digital surveillance network and its OPTera Metro portfolio to the MPS. JungleMUX is a state-of-the-art system for transporting surveillance video from a network of remote cameras back to a control centre. The OPTera Metro portfolio is the mainstay of Nortel's "Personal Internet" initiative, which is designed to enable Internet service providers to better track individual Internet users and their online activities, and thus heavily criticized recently by privacy advocates in the US.[52]

Nortel's presentation at Security China 2000 must have impressed someone. Shanghai Telecom (ST) recently announced that it had selected Nortel's OPTera product portfolio as a next-generation citywide fibre-optic broadband network. The contract estimated to be worth more than US$10 million means that Nortel will build China's first optical city network including a broadband access system and an ADSL solution for high-speed digital service to approximately 200,000 subscribers. The project is due to be completed in time to support Internet and video conferencing services for international media reporting the APEC Leaders' Meeting to be held in Shanghai in October 2001. Shanghai, powerhouse of the new Chinese economy, will be able to boast one of the most advanced citywide networks in the world.

The OPTera package is at the heart of Nortel's Personal Internet strategy and has allowed Shanghai Telecom to build an advanced parallel optical network supporting streaming media and other time critical transactions. Media streaming is very difficult to achieve over conventional Internet circuits. While Nortel's state-of-the-art fibre-optic links will dramatically increase the bandwidth available to the city, that is not the feature that stands out for anyone looking to increase security in the face of new, increasingly sophisticated threats to China's network security. Important components of the OPTera portfolio and key to the Personal Internet strategy are Nortel's Shasta and Alteon products[53], which will enable Shanghai Telecom to offer customized Web services to businesses and consumers. Nortel's "Personal Internet" strategy is all about personalizing content delivery services with a user-aware, content-aware network. This means that the network is designed to "think," that is to identify individual subscribers when they log on, matching names to IP addresses, and learning over time what content interests the subscriber.

> "Imagine a network that knows who you are, where you are, and can reach you whether you're on your mobile phone or at your desktop. Even better, imagine instead of finding your Web content, it finds you. Sounds personal. Exactly."[51]
>
> **– Nortel Networks, Personal Internet Strategy**

The Shasta 5000 BSN is designed to power the subscriber edge of the network, where "last mile" technologies like high-quality DSL meet the Internet backbone, and where broadband subscribers meet broadband services and content. Shasta is a universal aggregation point where conventional dial-up, DSL, fixed and mobile wireless, ATM/frame relay, and leased line connections all join the Internet. Shasta appeals to ST as a means to increase competitive advantage by becoming a value-added broadband services network. It appeals to Shanghai's Public Security Bureau (PSB), the most advanced of China's online police, because of a number of unique security properties it incorporates.

The Personal Internet strategy is presented to ST, as it is in the West, as a means to derive increased profits from its networks by, for example, offering security services or reselling data

to other companies. This practice of reselling personal data, criticized by many privacy advocates, is explicitly ruled out in Nortel Networks own Privacy Statement. Nevertheless, the Personal Internet strategy depends on the network's ability to match IP addresses to users' demographic profiles.

Nortel believes that its Personal Internet strategy is the key to the future of the Internet, and has put the Personal Internet at the center of its latest publicity drive. It is remarkable that Nortel can enthusiastically promote business practices to other corporations that it claims to avoid in its own operations.

Nortel's Personal Internet strategy enables Shanghai's PSB to move beyond simply tracking Web hits to targeting specific audiences, and creating demographic profiles in real time. Such intelligent network distribution and delivery has a profound impact on user privacy. "Personal Internet" is a network that always "knows who you are."

Internet users coming onto the network via a range of broadband access technologies such as DSL, wireless and cable have security settings applied to them on a per subscriber basis. With an extraordinary level of packet processing, Shasta is one of the most powerful carrier-class platforms for managing network security. Mass market broadband introduces new security concerns with "always on" Internet connectivity. The Shasta 5000 BSN provides extensive firewall capabilities that are simple to provision, and enable constant monitoring of every individual's traffic flow.

"Nortel Networks will not sell, rent, or share this information with any other organization."[54]

"Nortel Networks collects IP addresses for system administration and internal tracking. When you visit our site, our servers log the IP addresses only. We do not link IP addresses to anything personally identifiable."[55]
– Nortel Privacy Strategy, 2000.

Broadband access contrasts with traditional dial-up access, where subscribers dial in through their Internet service provider (ISP), conduct their business, and then log off. The transitory nature of dial-up access provides a limited window of opportunity to exploit any security holes. Therefore, security incidents with dial-up access are limited and have not been widely reported.

On the other hand, businesses with dedicated access connections (T-1, frame relay) are protected, but the high cost of these dedicated connections has made them less viable for the small and medium business markets and particularly for individuals, community groups and non-governmental organizations. Broadband connections are always on and permanently connected to the Internet. Yet today, most DSL and cable subscribers are connected to the Internet without firewalls and are therefore highly vulnerable. This issue poses a real threat to network security.

To counter this, Nortel's Shasta offers a layer of security positioned between personal firewalls and much more expensive corporate solutions. This security integrates an advanced policy-based state-aware firewall capability, with remote authentication, activity logging, encryption, and content filtering. Shasta's position at the edge of the network enables the service provider to apply security policies across each and every subscriber through one simple interface, rather than allowing subscribers to manage their own security.

The "subscriber edge" is the aggregation point in the service provider's network where the subscriber meets the network. It is the only point in the network where the service provider has complete knowledge, control and visibility of the subscriber and his or her traffic flows. Beyond this point, traffic from multiple subscribers gets aggregated over high-speed connections to backbone or core routers. Once traffic reaches the international gateways it lacks the transparency that affords monitoring agencies visibility into each individual subscriber's traffic flows.

Nortel's security solution reflects this principle: "the only viable point in the network where the service provider can apply any effective form of control over the subscriber's traffic is at the subscriber edge." In other words, while security software is located in the subscriber's own PC, it is managed remotely by his ISP. This strategy signals the end of the failed "Great Firewall," in that the focus of surveillance and content control is now on traffic at the edge of the network, rather than the centre – the international gateways.

Another significant feature of Shasta's security is its sophisticated anti-spoofing technology. Spoof attacks involve sending traffic that appears to originate from a legitimate source IP address and is therefore acceptable to the firewall, but the source address has been hijacked and used illegitimately. Even the most advanced firewalls can be and have been spoofed by the serious hacker. The Shasta 5000 BSN can prevent spoof attacks from getting through to the subscriber's network as it incorporates advanced anti-spoofing capabilities that can be applied to each individual subscriber. The Shasta 5000 BSN firewall filters traffic going to and from the subscriber, and prohibits the end-user from generating spoofed packets and from forwarding other subscribers' traffic.

This impacts on a number of areas. While it offers improved defences against distributed denial-of-service attacks, it also presents a challenge to systems that have been created to assist those trying to circumvent China's firewalls. This includes dissidents and democracy activists.

Service providers use identity verification in order to validate users requesting access to their networks. The authentication mechanisms will take many forms. Authentication mechanisms include, but are not limited to, user name and password, smart cards, and biometric devices such as fingerprint scanners or face recognition systems.

The Shasta 5000 BSN supports several forms of user authentication, dependent upon the access mechanism and protocol. For administrator access to the Shasta 5000 BSN, authentication is currently password-based but is designed to be compatible with biometric authentication in the future.

Activity logging helps track activities within and at the edge of a network to determine if rejected traffic represents a threat or forms a pattern. Such information can later be used to enhance the security features of the network and track specified "illegitimate" users.

The Shasta 5000 BSN provides an easy-to-use graphic user interface (GUI) for the creation and definition of full activity logging. With this service, the Shasta provides a log manager that displays every logged event per individual subscriber and per service. The log information is stored and delivered to remote databases. All events, including acceptance and rejection of packets, can be recorded in a log based on actions specified within the system and are time-stamped at the moment they are generated. All packets that are dropped due to non-conformance of a protocol's "normal" behaviour can also be logged in the log manager for later analysis.

Shasta's log manager enables the analysis, filtering and searching of the log in a variety of different ways, so that very detailed information about an individual's communication habits can be extracted quickly and efficiently. This information can then be stored in huge local and centralized databases for subsequent analysis by the MPS. In this way, for example, the MPS can match "real world" events to patterns within Internet traffic. An unusual surge in the number of e-mails sent the day before a demonstration, for example, would yield a lot of intelligence without even accessing the content of the messages.

Content filtering is another way to control incoming Internet content into any environment – home, school, cybercafé and business. Such filtering is done through predetermined filters used to block URLs meeting certain predefined criteria or categories for the particular environment or circumstance. Regional centres for Internet security under the control of the MPS, dedicated to maintaining such URL lists, are springing up throughout China to facilitate the government's information control strategy at a more local level.

Filtering is administered through a proxy in which an individual's Web requests are sent to a proxy server which checks requests against a list of "denied" URLs and blocks any incoming content from those URLs not meeting the Chinese government's predetermined criteria for "wholesome" Web content. The Shasta 5000 BSN has the ability to support just such proxy services through its redirection capability to such content filtering server sites. Through the Shasta 5000 BSN policy-forwarding capability, rules can be established to forward the subscriber traffic to content filtering servers, which then do the filtering on behalf of the government.

Locating content control at a more local level has two important consequences for anyone within China attempting to access information on the MPS' list of forbidden URLs. First it will become significantly more difficult to access such proscribed Web sites in the first place as

Shasta's firewalling capabilities are so much more sophisticated being located at the point where the user joins the Internet. For example, the practice of using proxy servers situated outside of China, currently prevalent among dissidents as a means of circumventing firewalls at the gateway level, will be much easier to detect and log – generating a pattern of use that will, over time, appear suspicious to the network.

Secondly, by assigning responsibility at a regional level for content filtration management, local MPS bureaus will be much more involved in the process of leveraging surveillance data from high-tech sources, and applying it to more low-tech scenarios – integrating Internet data with traditional modes of MPS surveillance, like networks of informers. This process is unmanageable at a centralized level except for the most high-profile cases, but becomes a potent means of control when distributed to regions, cities, and local neighbourhoods.

A Network That Knows Who and Where You Are

Right to Association

Everyone has the right to freedom of peaceful assembly and association.

The Universal Declaration of Human Rights, Article 20

One of the stated objectives of the Golden Shield project is the establishment of a nationwide network of closed-circuit television or CCTV cameras in public spaces to improve police response times to outbreaks of social unrest.[57] The incredible range of surveillance cameras on display at Security China 2000 indicates the extent to which technology is more complex today than years ago. New circuits allow the camera to ignore bright, light-emitting objects within its fields of view; miniaturization allows easier concealment; infrared cameras allow surveillance in darkness.

"The China CCTV market is worth US$350 to US$400 million per year," estimated Gerrit Hurenkamp, Development Manager for the US-based Pelco International. "It's a good market but difficult to get into. They are well educated here and know what they want. You can't just dump any product."

As video surveillance electronics become increasingly sophisticated ever-greater bandwidth is required to transport the stream of images produced from remote locations to control rooms. Such a system requires advanced network architecture, capable of spanning a country as large as China, and Nortel's presentation of its JungleMUX system at Security China 2000 spoke directly to that need. Closed-circuit video signals in Nortel's JungleMUX network are transported over a wide area network (WAN) operating between 1.6 to 44 Mbps and accessible by all the nodes in the network. Each video source (camera, VCR, etc.) is digitized using a user-configurable compression algorithm. This provides an efficient and scalable CCTV transport solution.

Recording can be in several modes: real-time, of varying qualities, and time-lapse. Real-time is like regular TV (at 30 frames per second, showing full motion). Time-lapse selects only a few frames per time period to record. The main advantage of time-lapse is that it allows one tape

Box 3:

"Neutral" Technology at Tiananmen Square

Following the Tiananmen Square massacre in 1989, the Chinese authorities tortured and interrogated thousands of people in an attempt to identify the demonstration's organizers. But even if the students and workers had resisted the terrors of the secret police, the hapless demonstrators stood little chance of anonymity. Stationed throughout Tiananmen Square is a network of UK manufactured surveillance cameras, designed to monitor traffic flows and regulate congestion. These cameras recorded everything that transpired in the months leading up to the tanks rolling into the square.

In the days that followed, these images were repeatedly broadcast over Chinese state television. Virtually all the transgressors were identified in this way. Siemens Plessey, which manufactured and exported the cameras, and the World Bank, who paid for their installation, claim they never had any idea that their "technologically neutral" equipment would be used in this way. However, in 1995 the World Bank authorized the funds to set up the same traffic flow system in Lhasa, the capital of the Tibet Autonomous Region. Lhasa is not, as yet, known for having problems with traffic congestion; besides, the area in which the traffic flow system is in operation is solely for pedestrians.[56]

to record for a much longer time than real-time recording, a particularly useful feature for archival purposes: high-resolution 700x480 colour pictures at 2 frames/sec, using about 400 kbps per camera. The flexibility in bandwidth allocation of JungleMUX Video Mapper allows for requesting higher resolution images and more frames per second from a specific camera, at any given time (up to broadcast-quality 700x480, 30 frames/sec NTSC colour signals, using about 6 Mbps [MPEG-2 quality]). The system even allows for ambient audio channels for public surveillance applications.

The revolution in urban surveillance will reach another level of control altogether – once reliable face recognition software becomes the norm. It will initially be introduced at stationary locations, like turnstiles, customs points, security gateways, etc., to enable a standard full-face recognition to take place. We are at the beginning of a revolution in "algorithmic surveillance" – effectively applying artificial intelligence routines to data analysis via complex algorithms, which enable automatic recognition and tracking. Such automation not only widens the surveillance net, it narrows the mesh.[58]

One company at the forefront of this revolution is AcSys Biometrics Corp., a joint venture between AND Corporation, inventor and developer of Holographic/Quantum Neural Technology, HNeT, and NEXUS, a diversified holding company. NEXUS is a Burlington, Ontario-based company operating through a highly diversified web of autonomous subsidiaries and partnerships.[59] AcSys is a provider of one of the most advanced facial recognition systems on the market. AcSys' Face Recognition System (FRS) is being incorporated into Nortel's own product portfolio. AcSys' FRS approach to security applies a proprietary technology for quick and reliable determination of human identity. It provides a scalable solution that integrates easily with existing systems and applications using standard network protocols.

In relation to Nortel's Personal Internet strategy, Rick Collins, Senior Manager of Nortel's "ProtoNet Project (Disruptive Solutions Implementation)," said of AcSys' FRS:

"Layering AcSys' face recognition's capabilities within Nortel Networks' solutions will make communication networks more personal. In the future, people may be recognized at a location, instead of logging in for some mobility services. I envision a network that knows who you are, and when you tell it, where you are, and can reach you whether you're on your mobile phone or at your desktop."[60]

AcSys Biometrics face and speech recognition system is based on a patented core of artificial intelligence called Holographic/Quantum Neural Technology (HNeT).

HNeT neural networks could power a range of Nortel's applications in the financial, manufacturing, security, surveillance, and medical sectors. With technologies like HNeT, with rates of learning up to 200 times faster than conventional neural nets, facial recognition via CCTV becomes a reality and countries with national CCTV infrastructures will view such technology as a natural extension of their networks. As with the example of the traffic control systems installed in Tiananmen Square and Lhasa, this process of extending a system's surveillance capabilities is one of subtle erosion of rights. The dynamics of this process: continuously upgrading technology and incorporating functions unintended by the design.

Diagram 1:

A New Model for the Internet: Innovation at the Edge of the Network

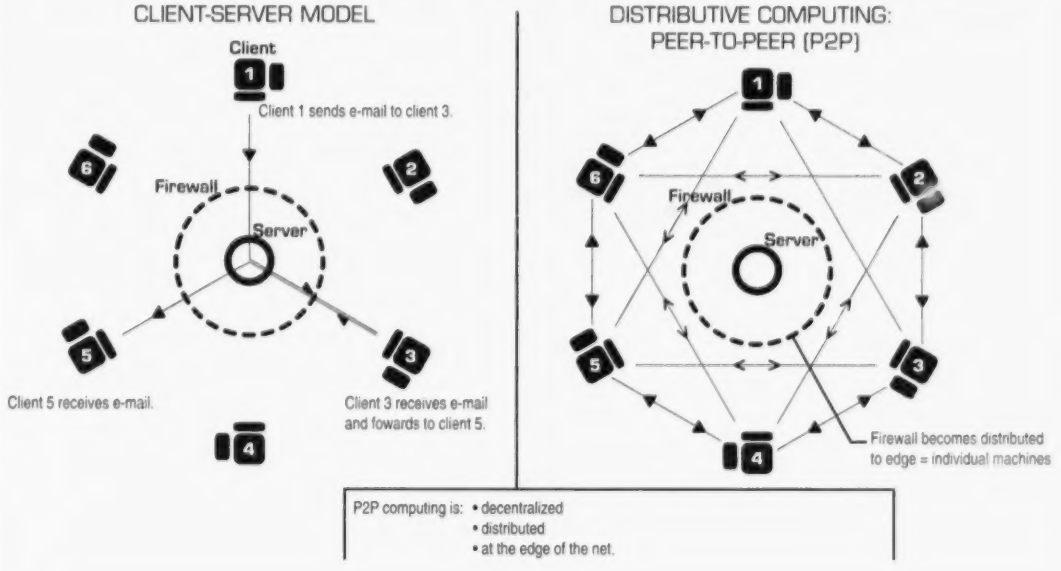
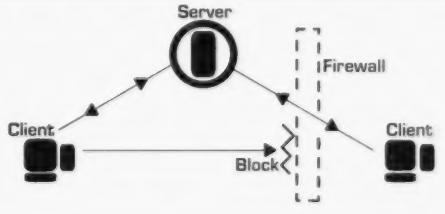


Diagram 2:

Interaction Across a Firewall

P2P software uses direct P2P communication by default. When a firewall makes direct interaction impossible, most P2P applications automatically send traffic to centralized relay service, where it is packaged as HTTP and "tunneled" through port 80.



Conclusion

"The mouse is mightier than the missile"

Democratic accountability is the only criterion that distinguishes Nortel's Personal Internet strategy, voice recognition research, or CCTV transport technology from advanced instruments of repression. In China, the concepts of "state security" and "state secrets," which are the foundation of regulations restricting Internet content and imposing obligations on service providers to monitor users, have routinely been used to punish free speech, block independent organizing and suppress information. In China, there are no privacy rights and government is not accountable through any legal process for the use of information obtained by its security apparatus via surveillance, wiretapping or online monitoring of electronic communication.

In China, as in every country around the world, human rights activists find themselves on the frontline of a new struggle to ensure that technological innovation works in favour of freedom and democracy and not for more and more subtle and sophisticated forms of repression. Many of the companies exhibiting their wares at the Security China 2000 Fair claim to share this objective, promoting their activities as "improving the quality of people's work and lives" (Philips) and "connecting anyone, anywhere, anytime... to the resources they need" (Sun Microsystems).

In practice, however, respect for fundamental human rights is required before such rhetoric rings of more than mere public relations spin. While the proponents of economic globalization flaunt the terminology of "level playing fields" and "rules-based systems," millions of people in China live within a system of political control that affects every aspect of their daily lives. There is no level playing field without freedom. There is no "rules-based system" when rules govern only the commercial dimension of human interaction. There is no freedom when the State routinely violates fundamental human rights.

Democratic governments, including the Government of Canada, must prioritize the promotion of human rights in all aspects of their international relations, including trade and investment. In its 1995 foreign policy statement *Canada and the World*, the Government of Canada affirms this commitment: "... we will make effective use of all of the influence that our economic, trading and development assistance relationships give us to promote respect for human rights."

In 1998 at a conference of non-governmental organizations in Montreal, then Canadian Minister of Foreign Affairs and International Trade Lloyd Axworthy said:

"Technology is changing the equations of power, challenging the conventional channels of communication, distributing and disseminating influence in the broadest possible fashion, to the point of democratizing the channels and getting rid of the gatekeeper... technology has a mind-boggling potential to break through barriers and overcome political obstacles to educate, inform and be an agent of political change... the mouse is mightier than the missile."[61]

Sadly, in China technology is serving no such lofty goals. Multinational companies pioneering the information revolution can no longer argue that their mere presence in China will guarantee increasing respect for human rights. Nor can governments cling to their arguments that open markets will lead automatically to democracy. Instead, in authoritarian and repressive countries where fighting crime is willfully confused with suppressing dissent, a different set of rules must be applied in order to shape political and social development. To ignore this challenge compromises freedom not only in China but in our globalized world, it compromises the freedom of all.

Appendix
How to Use the CD-ROM that Accompanies this Report

Installation:

The following instructions will help you install the CD-ROM for Windows 95/98/ME/2000 and MacOS.

1. Close all open programs on your computer and open your CD-ROM tray.
2. Place the CD-ROM in the tray, graphic side up.
3. When the CD-ROM is placed in the CD-ROM tray and the tray is closed, an autorun feature will launch the installation program.

If you do not have an autorun feature or have it disabled, you may launch the installation program named chinags.exe as follows:

Windows: Double-click the My Computer icon on your desktop. Double-click the icon that corresponds with your CD-ROM drive then double-click the icon labeled chinags.exe.

Mac: Click the CD-ROM icon on the desktop then click the icon labeled chinags.exe.

Liner Notes

> ***In an important sense, the means by which this report is distributed – particularly the Chinese language distribution – is as important as the content of the report itself.***

> **As a consequence of China's Internet legislation – particularly with regards to our obligation to provide access to mainland Chinese readers – and in the course of research and dissemination of this report, a number of open source tools and concepts have been employed. A brief outline of some of them appears below.**

> **If you are attempting to access the online version of this report (located at: go.openflows.org) from within the PRC, please make use of appropriate anti-censorship/anti-surveillance software as provided on the CD-ROM.**

> **On the Web site version and included on the CD-ROM you will find additional material related to the research process including an overview of Chinese legislation and regulations governing electronic communications.**

A Call to Action

At this year's Linux World Conference, Stanford University law professor Lawrence Lessig handed down a challenge to get involved and fight the powers of the "old."[62]

Lessig, famous for his work in cyber law and author of the book *Code and Other Laws of Cyberspace*, described how outdated legislation, big business, government and large corporations have co-opted the "free platform" of the Internet, one that ideally was designed to generate free expression, and instead have created something that stifles innovation.

"What do you want to do about it?" Lessig asked his audience. "I will have no effect stopping this change. The more I talk the less [government and corporations] want to listen, the less they want to hear this story. I'm useless in this battle. The people who can make the difference are you, the people who built this architecture of freedom."

Hacktivismo!

"Hacktivismo and the CULT OF THE DEAD COW are issuing the HACKTIVISMO DECLARATION as a declaration of outrage and a statement of intent. It is our Magna Carta for information rights. People have a right to reasonable access of otherwise lawfully published information. If our leaders aren't prepared to defend the Internet, we are."

"A Special Message of Hope," July 4, 2001[63]

Patrick Ball

"Hacktivism is using technology in the service of human rights," said Dr. Patrick Ball, the deputy director of the American Association for the Advancement of Science Human Rights program who has worked on United Nations human rights projects investigating war crimes and genocide as well as on projects in Guatemala, Haiti and South Africa, among others.

PGP

Many human rights groups use cryptography and encryption software such as PGP (Pretty Good Privacy) to protect their messages and information, which is often a matter of life and death. PGP, in its ability to keep information from falling into the wrong hands and to verify whether messages are authentic through the use of digital signatures, "has had an enormous impact on human rights." [See CD-ROM.]

Rubberhose

(pronounced Marutukku)

Rubberhose was originally conceived by crypto-programmer Julian Assange as a tool for human rights workers and journalists who needed to protect sensitive data in the field, particularly lists of activists and details of incidents of abuse.

The Rubberhose programmers met with human rights groups and heard first-hand accounts of such abuses. Human rights workers often carry vital data on laptops through the most dangerous situations, sometimes being stopped by military patrols who would have no hesitation in torturing a suspect until he or she revealed his or her passphrase to unlock the data.

Freenet

Freenet is a massive P2P network that pools the power of member computers around the world to create an archive open to anyone to freely publish or view information of all kinds. Version 1.0 of this report is published on Freenet in three languages, and is therefore available throughout China and the rest of the world. [See CD-ROM.]

SafeWeb

Internet in China Catalyst for Social Change?

SafeWeb is an SSL-encrypted anonymous proxy service that is currently used approximately 100 million times per month by hundreds of thousands of people worldwide, making it the most popular Web site in the world.

Triangle Boy is an open source program that lets volunteers turn their PCs into gateways into the SafeWeb network, thereby foiling attempts of restrictive governments to censor the Internet. Triangle Boy uses IP spoofing and packet routing technology to minimize the bandwidth consumption on volunteer machines. [See Diagram 2: Interaction Across a Firewall.]

Glossary

ADSL (Asymmetrical Digital Subscriber Line)

ADSL is used for moving data over regular phone lines. An ADSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. The ADSL circuit must be configured to connect two specific locations, similar to a leased line. ADSL allows downloads at speeds of up to 1.544 megabits (not megabytes) per second, and uploads at speeds of 128 kilobits per second.

Asynchronous Transfer Mode (ATM)/Frame Relay

A networking technology that contains a flexible multiplexing and switching technique which provides variable bandwidth for local area and wide area networks. Unlike ordinary synchronous configurations, ATM permits flexible allocation of available bandwidth for data, voice, images and video. ATM uses a scalable architecture, making it easily upgradable; it allows a virtually unlimited number of users to have dedicated, high-speed connections with high-performance network servers. Engineering studies indicated that ATM is theoretically capable of data rates of 622 Mbps over fibre optic and 155 Mbps over conventional copper.

Bandwidth

Literally, the frequency width of a transmission channel. Often used as an expression of the amount of data that can be sent through a circuit. The greater the bandwidth, the greater the amount of data that can travel in a given time period.

How much can you send through a connection? Usually measured in bits per second. A full page of English text is about 16,000 bits. A fast modem can move about 15,000 bits in one second. Full-motion full-screen video would require roughly 10,000,000 bits per second, depending on compression.

"Black Box"

A device Internet service providers fit to their servers that relays a copy of all data sent through the system to the state security service.

Broadband

When the bandwidth of a signal is large, it can simultaneously carry many channels of information. Fibre optic cable, in particular, has very high bandwidth, and is referred to as broadband.

Carrier

A telecommunications company that resells communications services to other businesses.

Carrier-Class

A modifier describing network equipment that has the high standards of reliability levels required to serve Internet service providers (ISPs). Carrier-class equipment usually offers at least 99.999% levels of reliability.

CDMA (Code Division Multiple Access)

A digital mobile wireless access protocol used for voice and data. It is being deployed worldwide and is based on spread spectrum technology. Datang has developed a Chinese version of the protocol: TD-SCDMA.

Compression (Algorithm)

Compression is a technique to make a file or a data stream smaller for faster transmission or to take up less storage space.

An algorithm is a formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clearly defined end point.

One everyday example of an algorithm is a recipe for baking a cake. Inventing elegant algorithms – algorithms that are simple and require the fewest steps possible – is one of the principal challenges in programming.

Convergence

The merging of two or more disparate disciplines or technologies. For example, the "fax revolution" was produced by a convergence of telecommunications technology, optical scanning technology, and printing technology. In a broader sense (New Media) convergence often refers to the merging of broadcast television, the Internet, and the personal computer.

Fibre optic

Light transmission through flexible transmissive fibres for communications

Filtering (Packet)

Controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or stopping them based on the Internet Protocol (IP) addresses of the source and destination. Packet filtering is one technique, among many, for implementing firewalls.

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques:

> **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is highly susceptible to IP spoofing.

> **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

> **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Gateway

Also known as application proxy, an application gateway is an application program that runs on a firewall system sitting between two networks. When a client program establishes a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This creates two connections: one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected. While this is considered a highly secure method of firewall protection, application gateways require great memory and processor resources compared to other firewall technologies.

Gbps

Short for gigabits per second, a data transfer speed measurement for high-speed networks such as Gigabit Ethernet. When used to describe data transfer rates, a gigabit equals 1,000,000,000 bits.

"Intelligent Buildings"

Intelligent buildings use electronics extensively to manage

> energy efficiency

> security systems

> telecommunications systems

> workplace automation

The ultimate dream in the design of an intelligent building has always been to integrate the four operating areas into one single computerized system. All the hardware and software would be furnished by a single supplier.

IP

Abbreviation of Internet Protocol. IP specifies the format of packets, sometimes called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time. The current version of IP is IPv4. A new version, called IPv6, is under development.

IP Addresses (Internet Protocol Number)

Sometimes called a dotted quad. A unique number consisting of four parts separated by dots, e.g. 163.113.245.2.

Every machine that is on the Internet has a unique IP number – if a machine does not have an IP number, it is not really on the Internet. Most machines also have one or more domain names that are easier to remember.

IP Spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted port. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted port and then modify the packet headers so that it appears that the packets are coming from that port. Newer routers and firewall arrangements can offer protection against IP spoofing.

Intranet, National or "China Wide Web"

A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use. As the Internet has become more popular many of the tools used on the Internet are being used in private networks, for example, many companies have Web servers that are available only to employees.

Mbps

Short for megabits per second, a measure of data transfer speed. Contemporary networks, for example, are generally measured in Mbps, which refers to one million bits per second.

Mux (Multiplexor)

Combines multiple signals (analogue or digital) for transmission over a single line or media. A common type of multiplexing combines several low-speed signals for transmission over a single high-speed connection.

Network

A group of two or more computer systems linked together. There are many types of computer networks, including:

> **local area networks (LANs):** The computers are geographically close together (that is, in the same building).

> **wide area networks (WANs):** The computers are farther apart and are connected by telephone lines or fibre optic.

In addition to these types, the following characteristics are also used to categorize different types of networks:

> **topology:** The geometric arrangement of a computer system. Common topologies include a bus, star, and ring.

> **protocol:** The protocol defines a common set of rules and signals that computers on the network use to communicate. One of the most popular protocols for LANs is called Ethernet. Another popular LAN protocol for PCs is the IBM token-ring network.

> **architecture:** Networks can be broadly classified as using either a peer-to-peer (P2P) or client-server architecture.

Computers on a network are sometimes called nodes. Computers and devices that allocate resources for a network are called servers.

Peer-to-Peer (P2P)

A type of network in which each computer has equivalent capabilities and responsibilities. This differs significantly from the client-server architecture, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally much simpler, but they usually do not offer the same system performance under heavy bandwidth loads. [See Diagram 1.]

Proxy Servers

A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Routing (Tables)

In internetworking, routing is the process of moving a packet of data from source to destination. Routing is usually performed by a dedicated device called a router. Routing is a key feature of the Internet because it enables messages to pass from one computer to another and eventually reach the target machine. Each intermediary computer performs routing by passing along the message to the next computer. Part of this process involves analyzing a routing table to determine the best path.

Smart Card

A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit (IC). Smart cards containing an IC are sometimes called integrated circuit cards (ICCs).

Smart cards are used for a variety of purposes, including:

> Storing a patient's medical records

> Storing digital cash

> Generating network IDs

Spam

Bulk unsolicited e-mail.

Streaming Media

A technique for transferring data such that it can be processed as a steady and continuous stream. Streaming technologies are becoming increasingly important with the growth of the Internet because most users do not have fast enough access to download large multimedia files quickly. With streaming, the client browser or plug-in can start displaying the data before the entire file has been transmitted.

TCP/IP

Transport Control Protocol/Internet Protocol, communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols also support TCP/IP.

Endnotes

[1] HONG KONG IS SWALLOWED UP, by Jeff Jacoby, *The Boston Globe*: http://www.bigeye.com/jj070197.htm
CHINESE CHECKERS, OxBlood Ruffin, CDC
http://www.cultdeadcow.com/cDc_files/cDc-0361.html
The Money Trap, A book review by Robert Kagan
Reprinted by permission of *The New Republic*
Originally published April 7, 1997
http://www.ceip.org/people/kagrep1.htm

[2] See endnote 59

[3] http://www.hrw.org/backgrounder/asia/china-bck-0701.htm. Freedom of Expression and the Internet in China, A Human Rights Watch Backgrounder

[4] Ibid, Dr. Stephen Hsu citing a CASS survey – Dr. Guo Liang, China Academy of Social Sciences, May 2001

[5] (CHINANET, CHINGBN, CERNET, CSTNET, and UNINET)
[See Diagram 1: A New Model for the Internet: Innovation at the Edge of the Network.]

[6] Translation of "churukou xindao"

[7] See, for example, http://www.wirednews.com/wired/5.06/china_pr.html
5.06 - June 1997, The Great Firewall of China, Geremie R. Barme and Sang Ye

[8] Big Brother Incorporated, Privacy International: http://www.privacy.org/pi/reports/

[9] http://www.cpsr.org/alert/cpsr.alert.2.05.html. Volume 2.05, November 12, 1993. Published by
Computer Professionals for Social Responsibility
Washington Office
(Alert @ washofc.cpsr.org)
Operation "Root Canal" Documents Released: Questions Raised about FBI's Digital Telephony Initiative
"In response to a CPSR Freedom of Information Act lawsuit, the FBI this week released 185 pages of documents concerning the Bureau's Digital Telephony Initiative, code-named Operation "Root Canal." The newly disclosed material raises serious doubts as to the accuracy of the FBI's claim that advances in telecommunications technology have hampered law enforcement efforts to execute court-authorized wiretaps."

[10] Original source:
http://www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html.
Nortel has subsequently removed this URL from its Web site. However, a copy of the original page remains in Google's Web cache and can be located here: http://www.google.com/search?q=cache:Ijjs4pWPJ8Y:www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html
"Nortel has been actively involved in ad hoc committees established prior to the law being enacted. We have been active participants during the standards process with technical representatives at key meetings."

[11] Final version (Enrolled Bill) as passed by both Houses:
http://thomas.loc.gov/cgi-bin/query/z?c103:H.R.4922.ENR: H.R.4922
To amend title 18, US Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other...

[12] Ibid, text from CALEA act

[13] http://www.askcalea.net/about/doj990914.htm
Department of Justice and FBI Reach First Agreement Under Communications Assistance for Law Enforcement Act

[14] http://www.askcalea.com/about/pl103414.htm
"(1) IN GENERAL – A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify."

[15] http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/1997013101.html
1997 B.C. Intell. Prop. & Tech. F. 013101
Government Tempers Electronic Surveillance Proposal; Critics Laud Changes But Are Not Satisfied
by Adam White Scoville, Staff Writer
See also: http://www.cdt.org/publications/pp_3.01.html
CDT POLICY POST Volume 3, Number 1, January 17, 1997

[16] See ENFOPOL timeline: http://www.heise.de/tp/english/special/enfo/6382/1.html.
See also: EU Document 496Y1104(01)
http://europa.eu.int/eur-lex/en/lif/dat/1996/en_496Y1104_01.html
"Whereas in accordance with a decision by the Trevi Ministers in December 1991 a study should be made of the effects of legal, technical and market developments within the telecommunications sector on the different interception possibilities and of what action should be taken to counter the problems that have become apparent..."

[17] The full text of all ENFOPOL documents cited in this paper can be found at http://www.statewatch.org/eufbi/index.html.
At the first meeting of the new Council of Justice and Home Affairs Ministers in Brussels on November 29 and 30, 1993, they adopted the following Resolution on "the interception of telecommunications" which speaks for itself, and is reproduced here in full:
"COUNCIL RESOLUTION ON THE INTERCEPTION OF TELECOMMUNICATIONS
The Council:
1. calls upon the expert group to compare the requirements of the Member States of the Union with those of the FBI;
2. agrees that the requirements of the Member States of the Union will be conveyed to the third countries which attended the FBI meeting in Quantico and were mentioned in the memorandum approved by the Ministers at their meeting in Copenhagen (Sweden, Norway, Finland [countries applying for accession to the European Community], the USA and Canada) in order to avoid a discussion based solely on the requirements of the FBI;
3. approves for practical reasons the extension to Hong Kong, Australia and New Zealand (which attended the FBI seminar) of the decision on co-operation with third countries which was taken at the Ministerial meeting in Copenhagen;
4. hereby decides that informal talks with the above-named countries may be envisaged: to that end the Presidency and the expert group might, for example, organize a meeting with those third countries to exchange information."

[18] See www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf:
SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA
DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE
OF ECONOMIC INFORMATION
Vol. 5/5: The perception of economic risks arising from the potential vulnerability of
electronic commercial media to interception

[19] http://www.oneworld.org/index_oc/issue198/codewar.html: The code war
David Banisar & Simon Davies. David Banisar is an attorney at the Electronic Privacy Information Center (EPIC) in Washington, DC and deputy director of Privacy International (PI). He is coauthor of a new book on encryption policy: *The Electronic Privacy Papers: The Battle for Privacy in the Age of Surveillance*. Simon Davies is director general of PI, the author of *Big Brother* and a visiting fellow at the London School of Economics.

[20] www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf

[21] http://www.statewatch.org/eufbi/index.html

[22] Draft COUNCIL RESOLUTION on the lawful interception of telecommunications in relation to new technologies ENFOPOL 19, March 15, 1999: http://www.fipr.org/polarch/enfopol19.html

[23] What do you want the Internet to be? http://www.nortelnetworks.com/corporate/internet/what_do_you_want/index.html

[24] China looks for new technology to police Net
By Martin Fackler, Associated Press, November 9, 2000

[25] http://www.adsaleexh.com/sec/press2.html
Press Release, August 29, 2000
Over 300 International Exhibitors Gather in Security China 2000
Taping the Lucrative China Market

[26] Ibid

[27] http://www.adsaleexh.com/sec/press1.htmmime text/html
Press Release, March 10, 2000
The No. 1 International Security Exhibition back to Beijing again

[28] Ibid, Adsale

[29] Ibid, Adsale

[30] Research Overview, Speech Signal Processing and Intelligence Technology Group Department of Electronic Engineering, Tsinghua University
http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm
Tsinghua has subsequently removed this URL from its Web site. However, a copy of the original page remains in Google's Web cache and can be located here:
http://www.google.com/search?q=cache:4EwAlksjbU:www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm+863+tsinghua+engineering+speech+continuous&hl=en

[31] Ibid

[32] http://www.most.gov.cn/English/Programs/863/menu.htm

[33] http://138.110.28.9/acad/intrel/chinmc.htm
EVAN A. FEIGENBAUM, "China's Military-Civilian Complex," *New York Times*, May 22, 1998

[34] Ibid, 27

[35] Ibid

[36] BNR operates and supports research laboratories at many sites around the world, including two in Canada (Ottawa and Montreal), three in the US (Raleigh, Richardson, and Atlanta), four in the United Kingdom (Harlow, New Southgate, Maidenhead, and Monkstown), one in Japan (Tokyo), one in Australia (Sydney), and one in China (Beijing).

[37] Nortel Networks Signs Contracts Valued At Over US$120 Million During Canadian Prime Minister Jean Chrétien's Visit to China
http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[38] http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm

[39] Specific compliance targets – known as J-STD-025 – establish standards for basic CALEA compliance: see Nortel's DMS-500 Series Platform, Document no: 51047-16-12-00.pdf.

[40] http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[41] Over US$100 million in the case of Nortel according to the US Dept. of Justice: see www.doj.gov.

[42] http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[43] According to a June 12 report in *China Daily*.

[44] http://www.smartcards-china.com/en/page_ehydt1.htm

[45] http://www.state.gov/www/global/human_rights/1999_hrp_report/china.html. Archive site for State Department information prior to January 20, 2001.
1999 Country Reports on Human Rights Practices
Released by the Bureau of Democracy, Human Rights, and Labor
U.S. Department of State, February 25, 2000

[46] Reported in Mingbao, courtesy of Judy Chen, HRIC

[47] http://www.telecomn.com/english/china_comm/CN_200010.htm. DATANG TELECOM CONTRACTS "INTELLIGENT BUILDING WEAK CURRENT ENGINEERING" FOR JILIN PROVINCIAL PUBLIC SECURITY DEPARTMENT

[48] http://www.gzjd.gov.cn/gzjd/

[49] Ibid, AP

[50] China online, http://www.chinaonline.com/topstories/001114/1/c00111456.asp

[51] http://www.nortelnetworks.com/corporate/leadership/personal/

[52] "The idea that ISPs are watching where [customers] go is unacceptable... it's like the Post Office looking into your mail in order to decide what kind of junk to send you." (Junkbusters.org) Several privacy bills are currently being introduced or reintroduced into the US Congress and state legislatures across the US. One bill being reconsidered by Congress, the Spyware Control and Privacy Protection Act, tries to protect online users from software like Nortel's Personal Internet technology. Of course, in China, spam and telemarketing are the least of Internet users worries.

[53] In addition to OPTera Metro, Nortel Networks solution for Shanghai Telecom includes Nortel Networks Shasta* 5000 Broadband Service Node (BSN) and Nortel Networks Passport* 15000 and Passport 7480 multiservice switches.

[54] http://www.nortelnetworks.com/help/legal/

[55] Ibid

[56] AN APPRAISAL OF THE TECHNOLOGIES OF POLITICAL CONTROL, An Omega Foundation Summary & Options Report For the European Parliament, September 1998

[57] Ibid 22 (AP)

[58] (See Norris, C., et. al, 1998.)

[59] Nexus (www.nxsgrp.com and www.nxs.ca), known formerly as Heritage Concepts International (HCI). NEXUS Group International Inc. AND Corporation (www.andcorporation.com). AcSys Biometrics Corp. (www.acsysbiometricscorp.com).

[60] http://www.andcorporation.com/press/press_3_12_01.html. AcSys Biometrics Accompanies Nortel Networks to CeBIT 2001.

[61] Bob Paquin, *The Ottawa Citizen*. Web posted Monday October 26, 1998, E-Guerrillas in the mist.

[62] Linux World Conference: http://www.linuxworld.com/

[63] http://www.cultdeadcow.com/cDc_files/declaration.html

"If you always stand straight,
then your shadow can never be crooked."
> Liu Qing, former political prisoner

Other Publications by Rights & Democracy:
(Visit our Web site at www.ichrdd.ca for a complete list of publications.)
A Human Rights Framework for Trade in the Americas, by Diana Bronson and Lucie Lamarche, 2001.
The Bilateral Human Rights Dialogue with China: Undermining the International Human Rights Regime, 2001.
Protecting Human Rights in a Global Economy: Challenges for the World Trade Organization,
by Robert Howse and Makau Mutua, 2000.
Canadian Mining Interests and Human Rights in Africa in the Context of Globalization, by Bonnie Campbell, 1999.
Women and Peacebuilding, by Dyan Mazurana and Susan McKay, 1999.
Putting Conscience into Commerce: Strategies for Making Human Rights Business as Usual, Volume 2, by Craig Forcese, 1997.
Human Rights: APEC's Missing Agenda, 1997.

Rights & Democracy

International Centre for Human Rights
and Democratic Development

1001 de Maisonneuve Blvd. East, Suite 1100 > Montréal (Québec) H2L 4P9
Tel.: 1 (514) 283-6073 > Fax: 1 (514) 283-3792 > E-mail: ichrdd@ichrdd.ca > Web site: www.ichrdd.ca

Droits et Démocratie
Centre international des droits de la personne
et du développement démocratique
1100 - 1001, boul. de Maisonneuve est, Montréal, QC, H2L4P9, Canada
www.ichrdd.ca – ichrdd@ichrdd.ca

CHINE : APERÇU DES ACTIVITÉS CANADIENNES DE PROMOTION DU COMMERCE ET DES DROITS HUMAINS.

Les échanges commerciaux avec la Chine : un marché en pleine croissance

La République populaire de Chine (à l'exclusion de Hong Kong) est le quatrième marché l'exportation du Canada (après les É.-U., l'UE et le Japon). En 2000, les exportations du Canada vers la Chine ont totalisé 3,7 milliards de dollars (une augmentation de 39,3 % par rapport à 1999) et les importations se sont élevées à 11,3 milliards, soit 26,4 % de plus qu'en 1999. Voilà donc un marché prometteur et en plein essor, que la Société canadienne pour l'expansion des exportations (SEE) qualifie de « seule demande décente en Asie ». La Chine constitue également la deuxième destination en importance des investissements directs dans le monde, dont 420 millions provenaient du Canada en 1999 (257 millions de plus qu'en 1994, mais comparativement à 3 milliards à Hong Kong). Le Canada envisage la négociation d'un accord bilatéral de protection des investissements avec la Chine (un APIE ou accord de promotion et de protection de l'investissement étranger).

Diplomatie : les intérêts économiques en tête de la liste de priorités du Canada

Sur le plan diplomatique, le Canada accorde une grande importance à la Chine. Il n'y a là rien d'étonnant, la Chine abritant presque le quart de la population mondiale ; mais à cela s'ajoutent de nombreux autres facteurs (histoire, immigration, liens culturels, etc.). Par conséquent, d'importantes ressources sont consacrées à la consolidation de la relation avec ce pays. Par exemple, entre 1998 et 2000, pas moins de 20 visites ministérielles ont eu lieu en Chine, notamment de la part du premier ministre, des ministres du Commerce international, des Finances, des Affaires étrangères, de la Défense, de l'Industrie, de l'Agriculture, des Ressources naturelles, de l'Immigration, des Travaux publics et du Revenu national ainsi que des secrétaires d'État pour l'Asie-Pacifique et des Sciences et technologies. Plusieurs autres personnages importants se sont rendus en Chine, notamment le chef de l'opposition, le chef des forces armées et la Juge en chef. Les hauts fonctionnaires chinois ont également visité le Canada à de nombreuses reprises.

Un certain nombre de questions ont été abordées lors de ces visites, mais la plus importante, comme le révèlent les portefeuilles des ministres qui se sont rendus en Chine, est l'intensification des liens économiques avec ce pays. Le problème n'est pas tant que le Canada ait augmenté ses échanges commerciaux avec la Chine, *mais plutôt le fait qu'on accorde beaucoup d'attention au commerce, alors que les droits de la personne semblent avoir dégringolé au bas de notre liste de priorités.* Les citoyens chinois qui luttent bravement pour le respect des droits humains – pour la démocratie, la liberté d'expression, les droits des travailleurs, soit le droit à la vie, à la liberté et à la sécurité – sont d'avis que leurs droits ont été sacrifiés par les gouvernements occidentaux qui se font concurrence afin de pénétrer le très convoité marché chinois.

Ainsi, on peut déplorer le déclin constant du soutien diplomatique accordé à la résolution sur les droits de la personne en Chine, comme on a pu le constater lors de la rencontre annuelle de la Commission des droits de l'homme de l'ONU ; cette situation coïncide avec l'augmentation des intérêts économiques occidentaux en Chine ainsi qu'avec les avertissements très explicites du gouvernement chinois contre toute « ingérence » dans les « affaires internes » de son pays.

Le gouvernement canadien et les entreprises canadiennes en Chine

La mission commerciale de février 2001 d'Équipe Canada a constitué la manifestation la plus visible de l'intérêt du gouvernement canadien pour le marché chinois ; elle était composée du premier ministre canadien, de huit premiers ministres provinciaux, de trois dirigeants territoriaux et de 800 gens d'affaires, ce qui témoignait d'un «

incroyable degré de soutien gouvernemental pour la communauté économique canadienne » (selon le Conseil commercial Canada-Chine). En fait, le gouvernement canadien s'emploie de multiples façons à promouvoir l'augmentation des échanges commerciaux avec la Chine et des investissements dans ce pays. Comparons les ressources consacrées au commerce avec celles vouées aux droits de la personne :

Commerce	Droits de la personne
Il existe des liens étroits entre l'ambassade canadienne à Beijing et les entreprises canadiennes exerçant leurs activités en Chine. Ex. : Howard Balloch, ancien ambassadeur canadien en Chine, est maintenant président du Conseil commercial Canada-Chine. De plus, les leaders politiques agissent régulièrement au nom du milieu des affaires. Un Site Web offre une foule de renseignements utiles aux entreprises.	Les droits de la personne sont tellement loin dans la liste des priorités que le simple fait d'en faire mention dans un discours vaut des félicitations au premier ministre ! Il n'y a aucun dialogue soutenu ou substantiel entre les ONG œuvrant à la défense des droits de la personne et le gouvernement à propos de la Chine.
Dans les bureaux du MAECI, dans d'autres ministères, dans les ambassades et les consulats, des centaines de fonctionnaires travaillent à l'augmentation des échanges commerciaux avec la Chine et aident les entreprises canadiennes à s'établir. Instructions détaillées sur les divers secteurs, relations d'affaires et conseils font partie de leurs activités quotidiennes.	L'équipe du MAECI chargée des droits de la personne compte au total 20 fonctionnaires, dont aucun n'est affecté au dossier des droits de la personne en Chine. Aucune aide comparable n'est offerte aux groupes de défense des droits humains qui travaillent sur la Chine.
Le gouvernement canadien publie fréquemment des rapports d'études de marché qu'il met gratuitement à la disposition des entreprises souhaitant investir en Chine ou entreprendre des échanges commerciaux avec ce pays ; ces rapports comportent de l'information à jour sur les plus récentes tendances du marché et les réglementations en vigueur en plus de fournir des listes de contacts en Chine et au Canada qui pourraient être utiles. Au cours des deux dernières années, plus de 30 rapports ont été élaborés sur l'aérospatiale et la défense, l'agriculture, l'alimentation et les boissons, les arts et l'industrie culturelle, l'automobile, les produits liés à la construction, l'équipement et les services liés à l'énergie électrique, les industries environnementales, la foresterie, l'industrie de la santé, les technologies de l'information et de la communication, les métaux, les minerais et l'équipement connexe, le pétrole et le gaz, les chemins de fer et le transport urbain, les services ainsi que l'industrie astronautique.	Très peu d'information a été publiée sur la position du Canada relativement aux droits de la personne en Chine. Les rapports sur le sujet élaborés par le gouvernement canadien sont demeurés confidentiels (tout comme ceux portant sur les autres pays). Une description de deux pages de la situation relative aux droits de la personne en Chine est généralement distribuée préalablement aux consultations des ONG sur les droits de la personne, qui ont lieu au début du printemps. Il arrive à l'occasion qu'un ministre publie un communiqué de presse ou émette dans un discours de timides commentaires sur les droits de la personne. Il n'existe pratiquement aucun document rendant compte du dialogue bilatéral tant vanté sur les droits de la personne en Chine.
Un soutien financier et des assurances, dont celles couvrant les risques politiques, sont offerts par différentes agences gouvernementales, notamment la Société pour l'expansion des exportations, la Corporation commerciale canadienne et l'ACDI Inc. Il est impossible d'obtenir des données précises quant aux projets ayant bénéficié d'un financement tiré des fonds publics. Le montant de l'appui financier accordé depuis 1995 par la SEE au secteur des hautes technologies de l'information et des télécommunications en Chine s'élève à 841,884,442.32 $	L'ACDI mène des projets bilatéraux relatifs aux droits de la personne en Chine portant sur la réforme judiciaire et d'autres aspects, qui exigent tous la collaboration du gouvernement chinois. Estimation totale pour 2000 : $ 11 millions.
Le personnel de l'ambassade organise des séances d'information personnalisées à quiconque en fait la demande deux semaines à l'avance.	Aucun arrangement de ce genre n'est offert aux personnes qui recherchent de l'information sur la situation des droits humains en Chine.
Le Groupe de consultations sectorielles sur le commerce extérieur (GCSCE) en matière de télécommunications et de technologies de l'information, qui agit à titre de conseiller auprès du ministre du Commerce international sur les intérêts des entreprises canadiennes dans le cadre des négociations sur le commerce international, est uniquement composé de représentants du milieu des affaires.	Les ONG œuvrant à la défense des droits de la personne sont invitées une fois par année à présenter des recommandations sur les droits humains en Chine à l'occasion d'une consultation s'échelonnant sur deux ou trois jours et portant sur l'ensemble des pays et des problèmes à l'échelle mondiale. Aucun groupe de défense des droits de la personne n'agit officiellement à titre de conseiller du Canada en ce qui a trait à ses rapports commerciaux avec la Chine.
D'importantes ressources sont consacrées à l'établissement de règles commerciales multilatérales favorables ; ainsi, il existe un solide soutien en faveur de l'admission de la Chine au sein de l'Organisation mondiale du commerce, de l'accord sur les technologies de l'information (ATI) et de l'accord sur les télécommunications de base dans le cadre de l'AGCS (Accord général sur le commerce des services).	Le Canada, à l'instar de nombreux autres pays occidentaux, a renoncé au système multilatéral de protection des droits de la personne en faveur d'un dialogue bilatéral dont les résultats sont plutôt douteux.

Qu'en est-il du secteur des télécommunications et des technologies de l'information ?

- L'ambassade canadienne à Beijing publie un bulletin relatant les derniers développements dans ce secteur ; ce bulletin comprend des conseils destinés aux entreprises canadiennes ainsi que de l'information à jour portant sur les questions juridiques et le marché.

- Au cours des cinq dernières années, dans le domaine des technologies de pointe et des télécommunications, la Société pour l'expansion des exportations a versé 841 884 442,32 $ en financement à court terme ainsi qu'à moyen et à long terme comprenant une assurance à court terme sur le commerce intérieur et l'exportation de même qu'une assurance-risques politiques, une assurance contractuelle et des produits de cautionnement. Il n'existe aucun mécanisme de contrôle de l'usage qui est fait des exportations de technologie soutenues par la SEE. Certains projets auraient été refusés parce que jugés incompatibles avec le respect des droits de la personne et de l'environnement, mais la SEE refuse de publier une liste détaillée des projets ayant bénéficié d'un financement ou d'une assurance, et ce, malgré sa nouvelle politique de divulgation d'information améliorée qui est entrée en vigueur le 1er octobre 2001.

- La Banque de Chine figure parmi les principaux emprunteurs de la SEE en Chine. La SEE a également des relations et des ententes avec la State Development Bank of China, la Export-Import Bank of China et la Industrial and Commercial Bank of China, qui appartiennent toutes au gouvernement chinois.

- John Roth, ancien chef de la direction de Nortel, a dit de la SEE : « Je n'ai qu'un conseil à donner : ne la changez pas trop. Il est inutile de réparer ce qui fonctionne déjà bien. »

- Entre 1992 et 1998, Nortel a fait don de 357 447,04 $ au Parti libéral du Canada.

Droits et Démocratie
Centre international des droits de la personne
et du développement démocratique
1100 - 1001, boul de Maisonneuve est, Montréal, QC, Canada
www.ichrdd.ca -- ichrdd@ichrdd.ca

La législation nationale et les règlements de la Chine relatifs à Internet

La législation et les règlements de la Chine régissant Internet reposent sur le principe d'« ouverture prudente » dans le but de préserver les avantages économiques de l'accès à des réseaux d'information mondiaux tout en protégeant le pays contre la domination économique étrangère et l'utilisation d'Internet par des groupes internes ou étrangers à des fins subversives. Bien que les chercheurs fassent souvent allusion à une stratégie Internet nationale, dans la réalité, le gouvernement de la Chine ne s'est doté d'aucune stratégie «officielle» articulée. Le présent document constitue une synopsis des politiques et des règlements connexes sur la sécurité d'Internet adoptés par différents groupes bureaucratiques.

En Chine, l'appareil de la sécurité de l'État regroupe toutes les organisations responsables de la sécurité interne et externe. Les deux plus importantes sont le Bureau de la Sécurité publique (BSP), responsable de la sécurité interne, et le ministère de la Sécurité de l'État (MSE), qui s'occupe de la collecte de renseignements civils étrangers et du contre-espionnage pour neutraliser les menaces provenant de l'étranger.

Depuis que la Chine a entrepris de moderniser son infrastructure de télécommunications, le BSP et le MSE en sont venus à revendiquer tous deux la réglementation de la sécurité d'Internet; en raison du caractère mondial d'Internet, il est en effet difficile de faire la distinction entre contrôle interne et contrôle externe.

Les enjeux sont élevés pour le gouvernement, alors que la Chine se joint à l'économie mondiale, et pour le «cyberdissident» potentiel, qui risque la peine de mort pour avoir utilisé Internet illégalement. L'environnement bureaucratique de la sécurité de l'information, très complexe, est marqué par les luttes continuelles pour la juridiction et l'autorité.

Le Bureau de la Sécurité publique

Le BSP est responsable du maintien de la sécurité du réseau civil, physique et en ligne, de la Chine. L'unité de première ligne du BSP, le Bureau de la supervision et de la gestion des ordinateurs, a été fondée dès 1983. Les règlements de gestion et de protection, réseau informatique et sécurité d'Internet *(Computer Information Network and Internet Security, Protection and Management Regulations)*, approuvés le 11 décembre 1997 par le Conseil d'État, stipulent clairement ses fonctions.

Depuis 1997, le BSP doit assurer la surveillance des fournisseurs de services Internet (FSI) et de toute autre entreprise commerciale comptant des employés qui ont accès à Internet. Conformément à l'article 8, les groupes et les personnes

engagés dans le commerce de services Internet doivent accepter de se soumettre à la surveillance, aux inspections et aux recommandations du BSP. Celui-ci exige des FSI qu'ils lui fournissent des rapports mensuels sur le nombre d'utilisateurs, le nombre de pages vues et les profils des utilisateurs. Ils doivent collaborer aux enquêtes du BSP concernant les violations de la loi et les activités criminelles impliquant des réseaux informatiques. Le FSI doit voir au maintien de la sécurité et toute violation par un utilisateur entraîne l'annulation de la licence d'exploitation du FSI et de l'enregistrement de son réseau, des amendes et possiblement de poursuites contre le personnel de l'entreprise et l'utilisateur (articles 20 à 23).

Pour éviter ces sanctions, les FSI ont donc mis en œuvre une série de politiques d'autocensure. Des *da mama*, employés rémunérés des FSI, dirigent des «armées» de volontaires qui patrouillent les bavardoirs et les babillards électroniques et effacent tout commentaire politique inacceptable.

Les règlements définissent également les utilisations acceptables d'Internet. Les utilisateurs doivent s'inscrire auprès du BSP en remplissant un formulaire de demande qui permet d'associer leurs renseignements personnels à de l'information sur leur compte réseau. En vertu de l'article 13, les utilisateurs ne peuvent prêter ou transférer ces comptes à d'autres personnes. Une fois en ligne, ils ne peuvent utiliser Internet pour créer, reproduire, extraire ou transmettre de l'information :

1. incitant à enfreindre la Constitution ou les lois ou l'implantation de règlements administratifs;
2. incitant à renverser le gouvernement ou le système socialiste;
3. incitant à la division du pays, en attaquant l'unification nationale;
4. incitant à la haine et à la discrimination envers les nationalités ou à attaquer l'unité des nationalités;
5. qui est fausse ou qui déforme la vérité, qui répand des rumeurs, détruisant l'ordre social;
6. qui alimente les superstitions féodales, qui constitue du matériel suggestif à caractère sexuel, qui incite au jeu, à la violence ou au meurtre;
7. à caractère terroriste ou incitant au crime, insultant ouvertement des personnes ou déformant la vérité à des fins de diffamation;
8. portant injure à la réputation des organisations de l'État;
9. incitant à d'autres activités contre la Constitution, les lois ou les règlements administratifs.

Le BSP détient l'autorité d'établir les normes sur les produits de sécurité de l'information en Chine. Dès février 1987, il s'est penché sur la question de la certification de la technologie alors que le nouveau comité de gestion de la normalisation se chargeait des technologies pour les enquêtes criminelles, pour le contrôle de la circulation et pour les applications informatiques ainsi que la technologie et l'équipement pour la sécurité publique.

En vertu de la loi de 1997 sur la sécurité des réseaux, tous les produits de sécurité de l'information doivent être évalués au laboratoire d'essai du BSP à Tianjin, dont l'emplacement n'est toujours pas connu. Ce laboratoire était mentionné dans le matériel promotionnel du salon «China International Information Security Exhibition » tenu du 26 au 28 octobre 1999 et du salon « Security China Exhibit » de novembre 2000, deux événements commandités par le BSP. Grâce à ce contrôle sur les produits de sécurité Internet, la position du BSP est unique : elle mène inévitablement à une étroite collaboration avec les entreprises nationales et étrangères qui vendent ces produits. Ces affiliations sont apparemment directes et indirectes : acquisition pure et simple, contrôle de facto, alliance stratégique ou simplement surpervision de la certification et des approbations.

Construction d'un cadre de travail juridique

Au cours de l'année dernière, le gouvernement chinois a rapidement élaboré un cadre de travail juridique fondé sur les règlements adoptés en 1997. En moins d'un an, trois lois furent votées, toutes les trois fort détaillées.

La législation adoptée le 1er octobre 2000 régit la participation des investissements étrangers dans le secteur Internet et le contrôle des sites par leurs propriétaires. En vertu de ces lois, toute entreprise étrangère désirant investir dans ce secteur doit d'abord obtenir l'autorisation du ministère de l'Industrie de l'information. En outre, les gestionnaires des sites chinois sont responsables de la révision et de la censure du contenu publié sur leurs sites et, en cas de manquement aux règlements, risquent des amendes ou la fermeture.

Un nouvel aspect important de la loi est que les gestionnaires ou propriétaires de sites doivent signaler toute infraction aux autorités. Ils doivent aussi être en mesure de fournir les adresses des utilisateurs Internet qui ont visité leur site au cours des 60 derniers jours. Ce règlement renforce également l'interdiction de publier de l'information « subversive » sur Internet, surtout des documents qui incitent au racisme et à la discrimination, encouragent les superstitions féodales, répandent des rumeurs pouvant mener au désordre social ou miner la stabilité sociale, font la promotion de l'indépendance du Tibet ou de Taiwan ou à contenu obscène, pornographique, violent ou à caractère terroriste.

Le 6 novembre 2000 furent adoptées d'autres lois décisives sur le contenu des sites et des groupes de discussion chinois sur le Web. Elles stipulent que les sites ne peuvent publier que de l'information provenant des médias publics, c'est-à-dire du contenu censuré en vertu des contraintes de la propagande officielle. Ils ne peuvent publier de nouvelles provenant de sources étrangères à moins d'une autorisation officielle. Les propriétaires ou gestionnaires de sites Web sont tenus responsables de toute information subversive qu'ils publient. Ces mesures s'appliquent également aux groupes de discussion. Toute personne qui viole cette nouvelle loi, surtout les propriétaires de sites Web, est passible de sanctions administratives, d'amendes ou de

prison, selon la gravité de l'infraction. Cela signifie que les nouveaux portails, tels que Sohu.com, sont entièrement tributaires de la presse officielle de la Chine.

Une loi adoptée le 28 décembre 2000 énonce que la propagation de rumeurs, la diffusion de propos diffamatoires ou la publication de renseignements nuisibles et l'incitation au renversement du gouvernement ou du système socialiste ou à la division du pays sont considérées comme des cybercrimes ou de la cyberdissidence. Elle prévoit l'emprisonnement pour la promotion ou l'établissement de cultes religieux et la divulgation de secrets d'État. En janvier 2001, l'agence de nouvelles officielle Xinhua annonçait que quiconque participait à des activités d'espionnage comme le vol, le dévoilement, l'achat ou la diffusion de secrets d'État au moyen du Web ou par tout autre moyen risquait la peine de mort ou la prison pour une période allant de dix ans à la réclusion à perpétuité.

Le ministère de la Sécurité de l'État

Le mandat du MSE porte sur la collecte de renseignements civils étrangers et le contre-espionnage. Institué en juin 1983, le MSE assume en plus des fonctions de sécurité interne du BSP et du service d'investigation du Comité central du Parti communiste. Depuis, le MSE et le ministère de la Sécurité publique (MSP) se livrent une bataille bureaucratique permanente, amplifiée dans le secteur de la sécurité de l'information, où la distinction entre sécurité interne et sécurité externe est inévitablement obscure.

Pourtant le mandat du MSE est clair : déjouer les efforts des étrangers visant à miner la sécurité de l'information en Chine. Cependant, il recoupe le rôle du BSP, par exemple sur le plan de la sécurité du réseau national. En outre, le MSE croit que la neutralisation des plans de subversion est uniquement de son ressort, surtout au Tibet et à Xinjiang, alors que c'est le MSP qui surveille les fournisseurs de services Internet et les autres groupes qui facilitent le contact avec l'extérieur du pays. Résultat : les deux bureaucraties s'enlisent dans un bourbier, oscillant entre coopération et conflit, de nouveaux affrontements survenant à chaque nouvel incident interne ou nouveau progrès technologique important.

Le Bureau des Secrets d'État

Des structures organisationnelles très développées pour la protection des « secrets d'État » sont le lot d'un système autoritaire à parti unique. Le régime à Beijing ne fait pas exception. Il dispose d'un entrelacement sophistiqué d'unités axées sur le secret à tous les échelons du parti. La plus importante de ces unités: le Bureau des Secrets d'État (BSE).

Le BSE est directement responsable de la protection des secrets d'État pour toutes les organisations du gouvernement chinois et du parti. En vertu de la loi de la République populaire de Chine sur la protection des secrets d'État, un secret d'État désigne toute affaire qui touche à la sécurité et aux intérêts de l'État, y compris à la défense nationale, aux affaires diplomatiques, aux décisions sur la politique relative aux affaires d'État, à l'économie nationale et au développement social, aux partis politiques et toute autre affaire d'État que le Bureau des Secrets d'État juge bon de protéger.

Dans la réalité toutefois, beaucoup de renseignements apparemment sans importance, comme les revenus des entreprises, sont qualifiés en Chine de secrets d'État, et certains renseignements ont été classés secrets d'État rétroactivement afin de faire avancer les intérêts politiques d'une personne, d'une unité ou de l'État.

Le BSE a cherché à étendre sa juridiction sur le contenu d'Internet. En janvier 2000, il décidait d'appliquer la loi sur les secrets d'État à Internet. Les nouveaux règlements sur la protection des secrets d'État relative aux systèmes d'information sur Internet *(State Secrecy Protection Regulations For Computer Information Systems on The Internet)* interdisent formellement le raccordement direct ou indirect de systèmes informatiques contenant des secrets d'État à Internet ou à tout autre réseau d'information public. Ces règlements interdisent également le stockage, le traitement ou la transmission de secrets d'État sur Internet. Enfin, il est défendu de publier ou de transmettre des secrets d'État sur des babillards électroniques, dans des bavardoirs ou dans des groupes Usenet. Les propriétaires de bavardoirs portent le fardeau de la censure du contenu. S'ils y trouvent de l'information « manifestement fausse », ils doivent la supprimer. Ils sont également tenus de signaler tout contenu suspect. Les propriétaires de sites Web doivent faire l'objet de vérifications de sécurité informatique et les sites pour lesquels les mesures appropriées contre les violations de la sécurité n'ont pas été implantées sont fermés. En outre, les propriétaires de sites Web ne peuvent embaucher de cyberjournalistes pour la rédaction

de textes. Ils ne peuvent que publier le contenu fourni par les médias étatisés puisqu'il leur est défendu de publier sans permission de l'information inédite.

Conclusion

Les analystes ne sont pas du même avis concernant l'impact de ce torrent de nouvelles lois. Certains sont portés à croire que l'impact sera relativement mineur puisque les propriétaires de sites Web savent déjà que la fuite de secrets d'État sur Internet est une activité illégale, des règlements provisoires à cet effet étant en vigueur depuis 1998. Les webmestres exercent déjà l'autocensure, ne publiant que les vues politiques des sources officielles ou évitant ce type de contenu en se concentrant exclusivement sur les sports ou le divertissement.

D'autres croient que les nouveaux règlements sont impossibles à appliquer en raison du coût et de l'impossibilité de surveiller le volume exponentiel de données échangées sur Internet et de retracer les envoyeurs ou les destinataires. Il se peut qu'il soit possible techniquement de filtrer des mots clés et de lire les courriels, mais cela aura pour effet de ralentir les communications sur Internet et par conséquent le progrès, ce à quoi le secteur économique s'opposera vivement. Concurremment, beaucoup de propriétaires de sites Web chinois ont affirmé qu'il est inévitable d'avoir des règlements et que, en un sens, ceux-ci sont utiles à la normalisation des pratiques et à la création d'un certain ordre au sein de l'industrie. D'autres, toutefois, sont convaincus que les règlements sur le cyberjournalisme auront un effet désastreux sur certains portails Internet chinois dont le contenu dépend de leurs propres informations de presse et de celles d'autres fournisseurs.

Peu importe son peu d'impact direct dans certains cas, la nouvelle législation participera indirectement à réprimer le dynamisme des débats en ligne qui caractérisait les débuts d'Internet en Chine. En outre, les nouveaux règlements ralentiront l'innovation technique tandis que les interprétations de la loi se multiplieront et que les applications contradictoires pourront effrayer les investisseurs étrangers, minant les efforts de la Chine pour exploiter le potentiel économique d'Internet.

La Déclaration du mouvement Hacktivismo

Pour la liberté et pour un Internet libre de toute censure

PROFONDÉMENT PRÉOCCUPÉS par le développement rapide de la censure du réseau Internet q sociétés transnationales,

REPRENANT À NOTRE COMPTE les principes et objectifs énoncés dans l'article 19 de *la Déclar* savoir que "tout individu a droit à la liberté d'expression et d'opinion, ce qui implique le droit de ne de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idé soit", ainsi que dans l'article 19 du Pacte international relatif aux droits civils et politiques, qui stipul

> 1- Nul ne peut être inquiété pour ses opinions.
> 2- Toute personne a le droit à la liberté d'expression; ce droit comprend la liberté de recherch informations et des idées de toute espèce sans considération de frontières, sous une forme or tout autre moyen de son choix.
> 3- L'exercice des libertés prévues au paragraphe 2 du présent article comporte des devoirs sp peut en conséquence être soumis à certaines restrictions qui doivent toutefois être expressém :
>
> > a) Au respect des droits ou de la réputation d'autrui;
> > b) À la sauvegarde de la sécurité nationale, de l'ordre public, de la santé et de la mora

RAPPELANT qu'un certain nombre d'États membres des Nations Unies ont signé le Pacte internatio l'ont ratifié de façon à empêcher leurs citoyens de l'invoquer devant les cours de justice,

CONSIDÉRANT que ces États membres continuent délibérément de bloquer l'accès à des informati même si le Pacte international énonce clairement que la liberté d'expression s'applique à tous les mé

PRENANT NOTE du fait que les sociétés transnationales continuent de vendre des technologies d'i de la planète,

ET PAR CONSÉQUENT CONVAINCUS que la communauté internationale des "hackers" a l'impé CE QUI SUIT :

• Le plein respect des droits humains et des libertés fondamentales inclut le droit à un accès équitabl par la radio à ondes courtes, le courrier par avion, la téléphonie ordinaire, le réseau Internet ou tout a

• Nous reconnaissons aux gouvernements le droit d'interdire la publication, entre autres, de secrets d infantile et de questions touchant à la vie privée et aux privilèges de la personne, mais nous nous op pour contrôler l'accès aux travaux et oeuvres des critiques, des intellectuels, des artistes ou des perso

• Le fait que les États cherchent à censurer Internet érode la coexistence pacifique et civilisée, comp péril le développement socio-économique des nations.

• La censure gouvernementale d'Internet constitue une forme grave de violence organisée et systéma générer la confusion et la xénophobie, et tromper de façon répréhensible notre confiance.

• Nous allons explorer des stratégies et des moyens de circonvenir la censure gouvernementale d'Int riposter aux violations des droits à l'information.

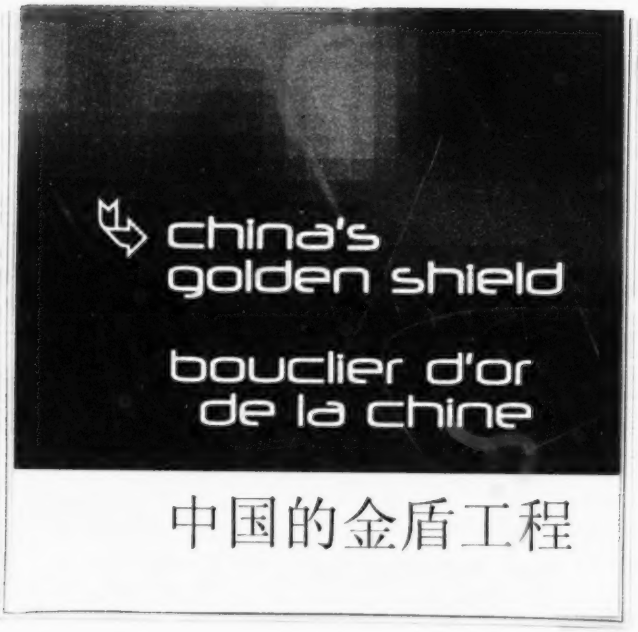
Le mouvement Hacktivismo et THE CULT OF THE DEAD COW
4 juillet 2001

bouclier d'or de la Chine

Les entreprises et le développement de la technologie de surveillance en Chine

entrer

par
Greg Walton


china's
golden shield
bouclier d'or
de la chine
中国的金盾工程

Droits et Démocratie est un organisme canadien investi d'un mandat international qui, en collaboration avec des organismes de la société civile et des gouvernements au Canada et à l'étranger, fait la promotion des droits humains et du développement démocratique par le dialogue, la sensibilisation, le renforcement des capacités et l'éducation du public. Droits et Démocratie articule son action sur quatre thématiques : le développement démocratique, les droits des femmes, les droits des peuples autochtones et la mondialisation et les droits humains ; ainsi que sur deux initiatives spéciales : la promotion des droits humains au plan international et les interventions d'urgence et occasions importantes.

L'auteur :
Greg Walton est un chercheur indépendant qui étudie surtout la question de l'impact des technologies et de la mondialisation sur les droits humains et la démocratie. Il travaille actuellement à mettre au point des « stratégies de conformité perturbatrices » pour des organismes sans but lucratif transnationaux. Sa page Web : go.openflows.org/jamyang.

Remerciements :
Carole Samdup, Diana Bronson et toute l'équipe de Droits et Démocratie. OxBlood Ruffin, cDc, Drunken Master et le projet Hacktivismo! y Oda, la cache Google, l'infrastructure Kundrel, SafeWeb, Patrick Ball, Jenny8, Wyrds of Simple Nomad, Openflows, M&D, et tant d'autres – de chaque côté du coupe-feu – qui bien sûr ont choisi de garder l'anonymat. Pour le moment. ;-)

© Centre international des droits de la personne et du développement démocratique, 2001.

Cette publication est gratuite. Toute citation du présent texte est permise à condition que l'origine en soit mentionnée et qu'un exemplaire de la publication où elle apparaît soit fourni à Droits et Démocratie.

Dépôt légal : Bibliothèque nationale du Québec, quatrième trimestre 2001.
Bibliothèque nationale du Canada, quatrième trimestre 2001. ISBN : 2-922084-43-4.

Graphisme : Laperrière Communication
Imprimé au Canada

Le Bouclier d'or de la Chine 1.0 est publié sur le site www.ichr.dd.ca et à titre de rapport libre sur les droits humains à : go.openflows.org.

LIBERTÉ_D'EXPRESSION : LIBERTÉ_DE_CODE

Toute personne a droit à ce que règne, sur le plan social et sur le plan international, un ordre tel que les droits et libertés énoncés dans la présente Déclaration puissent y trouver plein effet.

Article 28 de la Déclaration universelle des droits de l'homme

Selon Bill Gates, il est un peu étrange d'associer le libre-échange à des questions de droits humains : cela équivaut à s'ingérer dans les affaires internes.[1]

Bill Gates, alors chef de la direction de Microsoft,
aux côtés de Jiang Zemin au cours d'une séance de photos à Beijing, en 1994

Table des matières

Préface 4
Résumé 5
Introduction 8
Encadré 1 : Le prix de la liberté 10

Transfert des technologies et convergence des politiques 11
Opération Root Canal 12

Que voulez-vous que soit Internet ?
« Un contact humain. Je veux qu'il sache qui je suis. » 14
Le projet Bouclier d'or 15
Une alliance inconvenante 16
Encadré 2 : Les projets « Golden » de la Chine : « Modernisation » de l'économie de la Chine 17
Au-delà de la grande muraille électronique 18
Internet et la vie privée 20
L'extrémité abonné 22
Une ombre virtuelle 23
Un réseau qui sait qui vous êtes et où vous êtes 25
Encadré 3 : Technologie « neutre » sur la place Tienanmen 26
Diagramme 1 : Un nouveau modèle pour Internet : l'innovation à l'extrémité du réseau 27
Diagramme 2 : Interaction en présence d'un dispositif coupe-feu 27

Conclusion – « La souris est plus forte que le missile » 28

Annexe : Comment utiliser le CD-ROM qui accompagne le présent document 29
Textes de la pochette 29
Glossaire 32

Notes en fin d'ouvrage 36

Préface

On a souvent qualifié les nouvelles technologies de l'information et des communications d'élément moteur de la mondialisation. Elles ont aussi été promues comme étant un outil de démocratisation alors que la connectivité était proclamée comme marquant la fin des disparités technologiques. Il ne fait aucun doute que les communications électroniques ont facilité la circulation de l'information sur la planète ainsi que la construction d'un réseau de soutien international aux activistes luttant pour les droits humains et la démocratie.

Malheureusement, l'avènement des technologies modernes de communication a aussi lancé de nouveaux défis aux défenseurs des droits humains, surtout à ceux qui vivent dans des régimes répressifs. Dans un monde où les règles de commerce international n'ont aucun lien avec le droit international relatif aux droits humains, les priorités économiques menacent la promesse de démocratisation par les technologies. En Chine, où il n'existe ni responsabilité démocratique ni lois pour la protection des droits humains, les technologies peuvent devenir, et sont devenues, des instruments de répression.

Il y va du droit de tous les hommes à un ordre international dans le cadre duquel les promesses de la Déclaration universelle des droits de l'homme pourraient être tenues. La Déclaration, ainsi que le Pacte international relatif aux droits civils et politiques qui l'accompagne, vise à protéger les droits fondamentaux de la personne, y compris le droit à la vie privée. La protection des droits humains constitue une obligation des gouvernements et doit s'appliquer à toutes les activités de ces gouvernements, qu'il s'agisse de la promotion d'échanges commerciaux, de la négociation d'ententes commerciales bilatérales ou internationales, de financement à l'exportation ou d'aide au développement.

Le présent document montre à quel point les technologies de pointe, développées au Canada et mises de l'avant au moyen d'une série de processus nationaux et internationaux, peuvent miner les principes des ententes sur les droits humains. Le projet Bouclier d'or de la Chine menace la protection des droits de la personne, surtout le droit à la vie privée – un droit qui étaye d'autres éléments essentiels de la lutte pour les droits humains, comme la liberté d'association et la liberté d'expression. Le Bouclier d'or positionne l'alliance entre le gouvernement et les entreprises à l'opposé du cyberfront du mouvement de lutte pour le respect des droits humains en Chine.

Le présent document cherche à donner un aperçu du monde de la haute technologie, des grandes entreprises et de la lutte pour les droits humains et la démocratie en Chine. Au nom de Droits et Démocratie, je propose ce document dans un esprit de solidarité avec le peuple chinois, qui trouvera peut-être utile son contenu dans son développement et sa consolidation des mouvements sociaux pour le changement. Je l'offre également à tous mes compatriotes au Canada qui, à la lumière des récents rapports sur la surveillance policière des dissidents au Canada, pourront découvrir combien les droits des citoyens de la Chine sont étroitement liés aux nôtres.

Le président,
Warren Allmand, c.p., o.c., c.r.

Résumé

La Chine vit un paradoxe très moderne. D'une part, les dirigeants sont conscients que les technologies de l'information sont le moteur de l'économie mondiale et que la croissance économique de la Chine repose en grande partie sur l'intégration du pays à l'infrastructure mondiale de l'information. D'autre part, la Chine est un pays à régime autoritaire et à parti unique qui assure sa stabilité sociale par la suppression des activités antigouvernementales. En bref, le contrôle politique repose sur la croissance économique; celle-ci nécessite la modernisation des technologies de l'information, qui, à leur tour, peuvent affaiblir le contrôle politique.

La « grande muraille électronique de Chine » se fissure. Le gouvernement sait qu'il ne peut espérer purger l'information de tout matériel jugé « répréhensible » avant son entrée sur les réseaux de Chine. Tiraillée par ces forces contradictoires d'ouverture et de contrôle, la Chine cherche un équilibre entre les besoins en information de la modernisation économique et les exigences en sécurité pour une stabilité interne. Dans la recherche de cet équilibre, la Chine a trouvé des alliés de taille parmi les entreprises de télécommunications privées principalement en Occident. Nombreuses sont celles qui jouent un rôle déterminant dans la satisfaction des besoins en sécurité du gouvernement chinois, notamment Nortel Networks, jusqu'à tout récemment la plus grande entreprise au Canada. Nortel Networks et d'autres entreprises internationales aident en fait la Chine à remplacer sa grande muraille électronique érigée au niveau des passerelles internationales par un système plus évolué de filtrage du contenu au niveau de l'individu.

Les anciennes méthodes de censure sont en voie d'être supplantées par une architecture de surveillance massive et omniprésente : le Bouclier d'or. Le véritable objectif est d'intégrer une gigantesque base de données en ligne à un réseau de surveillance globale incorporant la reconnaissance de la parole et des visages, la télévision en circuit fermé, des cartes intelligentes, des dossiers de crédit et des technologies de surveillance d'Internet. Le FBI (Federal Bureau of Investigation) des États-Unis y prête main-forte par son ambitieux projet de normalisation de l'équipement de télécommunications pour faciliter la surveillance électronique, projet maintenant adopté comme norme internationale.

Nombreux sont ceux qui en Chine sont mis en état d'arrestation pour des « crimes » Internet, que ce soit pour avoir fourni des adresses de courrier électronique à des publications Internet ou pour avoir fait circuler de l'information en faveur du mouvement démocratique ou des articles dénonçant le gouvernement chinois, en contradiction flagrante avec le droit international relatif aux droits humains garantissant la liberté d'expression. Les dissidents sont en général accusés de « subversion » ou d'avoir « menacé de renverser le gouvernement », la distinction entre une activité criminelle et l'exercice du droit d'expression étant inexistante en Chine. Le développement de cette nouvelle architecture globale de surveillance électronique compliquera encore plus la vie de ces activistes courageux.

Le salon Security China 2000, tenu à Beijing, a attiré environ 300 entreprises de plus de 16 pays. Parmi les organisateurs : la « Commission sur la gestion de la sécurité publique du Comité central du Parti communiste chinois ». Au salon, le nouveau projet Bouclier d'or du ministère de la Sécurité publique a rapidement ravi la vedette. Son but : promouvoir l'adoption des technologies de l'information et des communications de pointe pour renforcer le contrôle policier central, améliorer les capacités de réaction, aider à mieux combattre le crime et rendre plus efficace le travail des policiers. L'appareil de sécurité de la Chine a de grandes ambitions : construire un réseau de surveillance numérique à l'échelle de la nation, permettant de relier les agences de sécurité locales, régionales et nationales dans un circuit de surveillance globale. Beijing voit le projet Bouclier d'or comme un système de télésurveillance fonctionnant à partir de bases de données avec accès immédiat aux dossiers d'enregistrement de chaque citoyen et des liens vers de vastes réseaux de caméras visant à améliorer l'efficacité des services de police.

Pour réaliser le Bouclier d'or, le gouvernement chinois s'appuie sur l'expertise technologique et les investissements des entreprises occidentales. Nortel Networks du Canada joue un rôle déterminant dans ce scénario comme le démontrent :

> ses projets de recherche en participation avec l'Université de Tsinghua pour l'adaptation de la technologie de reconnaissance de la parole à des fins de surveillance automatique des appels téléphoniques ;

> son appui d'emblée et précipité aux plans du FBI de mise au point d'une norme commune pour l'interception des communications téléphoniques, la CALEA, de concert avec le transfert technologique assuré par la coentreprise Guangdong Nortel (GDNT) ;

> son étroite collaboration avec Datang Telecom, une entreprise chinoise ayant des intérêts importants dans le marché de la sécurité publique en Chine ;

> la promotion du JungleMUX, qui permet le transfert des données vidéo d'un réseau de télésurveillance vers un centre de contrôle du ministère de la Sécurité publique (MSP) de Chine ;

> le déploiement de ses produits Internet Personnel à Shanghai, grâce auxquels les fournisseurs de services Internet peuvent beaucoup mieux surveiller les communications des utilisateurs ;

> un projet de 10 millions de dollars US pour construire un réseau optique large bande urbain (OPTera) à Shanghai permettant aux autorités de surveiller les activités des abonnés à l'extrémité du réseau, principalement au moyen du coupe-feu Shasta 5000, ce qui constitue une violation du droit à la vie privée. Il est donc de plus en plus difficile pour les

dissidents d'avoir des communications clandestines et de plus en plus facile pour la police de découvrir qui sont les utilisateurs d'Internet qui tentent d'accéder à des URL jugées non appropriées par le gouvernement chinois ;

> l'intégration des technologies de reconnaissance de la parole et des visages en collaboration avec AcSys Biometrics, une filiale de NEXUS à Burlington en Ontario.

Beaucoup d'autres entreprises occidentales ont participé au renforcement d'un appareil de sécurité répressif au moyen des développements suivants :

> une base de données nationale comprenant des données sur tous les citoyens adultes de la Chine ;

> des cartes intelligentes pour tous les citoyens, qui peuvent être lues à distance à l'insu du porteur ;

> un système de télévision en circuit fermé pour la surveillance des endroits publics ;

> la technologie qui permet au Bureau de la Sécurité publique des comparaisons instantanées d'empreintes digitales ;

> le développement de coupe-feu en Chine.

Le discours technologique actuel, préoccupé avant tout par la satisfaction de ses propres besoins, promet que les nouvelles technologies de l'information et des télécommunications seront démocratiques en soi et qu'elles favoriseront l'ouverture partout où elles seront employées. *Le Bouclier d'or de la Chine. Les entreprises et le développement de la technologie de surveillance en Chine* détruit ce mythe. La technologie fait partie intégrante d'un contexte social et, comme le montre le présent document, elle favorise la répression dans un régime à parti unique au nom de l'expansion des marchés et de profits exponentiels.

Introduction

Des télécommunications inadéquates ont depuis longtemps été le lot de la Chine. La croissance économique a exigé la modernisation d'une infrastructure caractérisée par une technologie désuète et un accès limité aux ressources nécessaires pour la développer. Pour pallier ces manques, le gouvernement s'est lancé dans un effort, bien financé, de modernisation de son infrastructure d'information. La Chine est donc devenue un des plus grands consommateurs d'équipement de télécommunications au monde.

Un objectif important de cette modernisation a été l'acquisition d'équipement de télécommunications évolué auprès des pays industrialisés, la révolution sur le plan des technologies de l'information étant perçue comme l'occasion pour la Chine de faire un pas de géant et de grandement améliorer ses capacités dans les secteurs liés aux télécommunications. Le transfert de ces technologies à la Chine a été facilité par deux tendances étroitement liées.

D'abord, les entreprises de télécommunications se livrent une concurrence féroce dans le partage du marché des télécommunications chinois, relativement peu développé mais à croissance rapide, mais surtout le plus grand marché au monde. De toute évidence, cette source potentielle de milliards de dollars attire les plus importantes entreprises de télécommunications, notamment Lucent et Cisco aux États-Unis, Nokia et Ericsson en Europe et Nortel Networks au Canada, sans compter toutes les autres. La Chine achète annuellement de ces entreprises plus de 20 milliards de dollars d'équipement de télécommunications.

La Chine représente environ 25 % du marché mondial de l'équipement de télécommunications, en pleine expansion exponentielle. Une grande partie de cette croissance est attribuable aux ventes d'équipement des entreprises de télécommunications étrangères et aux coparticipations avec des entreprises en Chine, ce qui nous amène à la deuxième tendance.

L'installation d'une infrastructure de télécommunications évoluée en vue de faciliter la réforme économique complique beaucoup les objectifs de sécurité interne du pays. Plus la quantité d'information circulant sur les réseaux de Chine augmente, plus il est difficile pour le gouvernement de contrôler cette information.

La croissance exponentielle d'Internet en Chine laisse croire à certains que les nouvelles technologies adoptées vont créer une société plus ouverte et plus démocratique. On se base sur l'hypothèse qu'Internet est en soi un moyen de démocratisation qui favorise le pluralisme, renforce la société civile et, de ce fait, force les gouvernements à rendre des comptes. Dans un monde d'après-guerre froide, le pouvoir des technologies de l'information et des communications de transformer les sociétés répressives est souvent considéré comme une évidence.

Pourtant, à la lumière des événements récents ayant eu lieu en Chine, le potentiel d'Internet comme moyen de démocratisation revêt un caractère improbable. La documentation à ce jour est éloquente : les dirigeants de la Chine ont résolument choisi de censurer le contenu en ligne et de restreindre l'accès des citoyens à l'information publiée à l'extérieur du pays.[3] Ils visent également à empêcher l'émergence de l'« organisation virtuelle » qui est devenue une importante fonction d'Internet dans les démocraties occidentales. Vu sous cet angle, Internet lance un certain nombre de nouveaux défis au régime. Selon un sondage récent mené par l'Académie chinoise des sciences sociales, 10 % des utilisateurs admettent utiliser régulièrement des

serveurs mandataires pour contourner la censure, la plupart des utilisateurs ont presque autant confiance dans les sources étrangères de nouvelles que dans les sources gouvernementales et la majorité croient qu'Internet aura un impact important sur la vie sociale et politique.[4]

Aux prises avec cette rapide transformation, les autorités chinoises sont impatientes d'acquérir les nouvelles technologies qui leur permettront d'augmenter la surveillance. Internet peut certes donner du pouvoir aux citoyens, mais il fournit également au gouvernement une nouvelle série d'outils de répression pour surveiller les échanges privés et censurer l'opinion publique.

En mars 2000, a Beijing, le president chinois Jiang Zemin (à gauche) serre la main de Frank Carlucci, president de Nortel Networks du Canada.

Dès le premier raccordement de la Chine au réseau Internet mondial en 1994, les autorités ont cherché à contrôler les liaisons Internet. Une restriction sévère de la connectivité internationale constituait le cœur de la stratégie de sécurité Internet naissante de la Chine. Aujourd'hui, sept ans plus tard, les connexions internationales des cinq réseaux principaux de la Chine sont desservies par des serveurs mandataires raccordés à des « passerelles »[5] internationales officielles. Le filtrage et la surveillance du trafic réseau s'effectuent toujours à ce niveau. Nommée par dérision la « grande muraille électronique »[6] par les pirates informatiques et les journalistes à l'échelle de la planète, cette stratégie a remporté un succès mitigé. En effet, la modernisation économique continuelle a entraîné une croissance exponentielle de la demande pour une largeur de bande internationale, et le volume actuel du trafic Internet pose un sérieux défi à la stratégie de censure par l'État au niveau des passerelles.

De nombreuses raisons expliquent la construction du réseau chinois sur ce modèle de « grande muraille électronique ». Les passerelles moduleraient le rythme de l'ouverture de la Chine au monde au moyen d'une interaction électronique. Le gouvernement pourrait décider à quel rythme augmenter les connexions et, en théorie, couper celles-ci en cas d'urgence sociale.

Les passerelles devaient constituer la première ligne de défense contre les intrusions antigouvernementales dans le réseau, une sorte de dispositif coupe-feu dont la fonction était de restreindre la quantité d'information sur les réseaux internes accessible aux intrus étrangers. Elles ont été conçues pour empêcher les citoyens de la Chine d'utiliser Internet pour accéder à des sites interdits et à de l'information antigouvernementale provenant de l'étranger. Les autorités espéraient, grâce à ce contrôle par l'État des tables d'acheminement au niveau des passerelles, empêcher les Chinois d'accéder à des sites étrangers comme ceux du Cable News Network (CNN), de la British Broadcasting Corporation (BBC), du Réseau d'information du Tibet (Tibet Information Network) ou de Human Rights Watch/Asia.

Les règlements et les lois de la Chine régissant Internet reposent sur le principe d'« ouverture prudente » dans le but de préserver les avantages économiques de l'accès à des réseaux d'information mondiaux tout en protégeant le pays contre la domination économique étrangère et l'utilisation d'Internet par des groupes internes ou étrangers à des fins subversives. Les enjeux sont élevés, pour le gouvernement alors que la Chine se joint à l'économie mondiale et pour le « cyberdissident » potentiel, qui risque la peine de mort pour avoir utilisé Internet illégalement.

Encadré 1 :

Le prix de la liberté

En janvier 2001, l'agence de presse officielle Xinhua annonçait que toute personne impliquée dans des « activités d'espionnage » comme « le vol, la pénétration, l'achat ou la divulgation de secrets d'État » au moyen d'Internet ou par tout autre moyen risquait la peine de mort ou une peine d'emprisonnement allant de dix ans à la réclusion à vie.

> Le 18 janvier 2000, Leng Wanbao était interrogé pendant trois heures après avoir fait circuler une lettre d'un autre dissident à l'extérieur de la Chine sur Internet. La police a rappelé à Leng Wanbao que l'envoi d'une telle lettre contrevenait aux lois sur la sécurité publique.

En 1998, Lin Hai, un entrepreneur en logiciels, est accusé de subversion pour avoir fourni des adresses de courrier électronique chinoises à un magazine Internet prodémocratique.

> Le 3 mars 2000, les autorités chinoises relâchaient Lin Hai, un entrepreneur en logiciels, qui avait été condamné à deux années de prison pour avoir incité des personnes « à renverser l'État ». Arrêté en 1998, Lin Hai était accusé d'avoir fourni 30 000 adresses de courriel chinoises à des publications dissidentes outre-mer, notamment *VIP Reference*. Les adresses ont servi à distribuer des articles dissidents sur Internet. Relâché dans le plus grand secret en septembre 1999, Lin Hai hésitait beaucoup à parler de sa situation, suggérant que les autorités l'avaient libéré plus tôt que prévu en échange de son silence. À sa sortie de prison, Lin Hai s'est qualifié de « premier prisonnier Internet chinois ».

> Le 3 juin 2000, Huang Qi, directeur du site www.6-4tianwang.com comprenant un forum de discussion, a été arrêté et accusé de « subversion », plus précisément d'avoir publié sur son site Web hébergé aux États-Unis des articles qui condamnaient le massacre de Tienanmen en juin 1989. Le site publiait une lettre de la mère d'un jeune étudiant tué durant le massacre ; celle-ci encourageait la reprise du mouvement prodémocratique de 1989. L'ordinateur de Huang Qi ainsi que tous les documents trouvés à son bureau et a sa résidence furent confisqués. Le site, ouvert à « tous ceux qui ont quelque chose à dire », est toujours maintenu par des Chinois dissidents vivant aux États-Unis, mais les utilisateurs d'Internet en Chine ne peuvent plus y accéder.

> Le 16 août 2000, la police interrogeait Jiang Shihua, un professeur en informatique de la province de Sichuan, dans le sud-ouest de la Chine. On l'accusait d'« incitation à la subversion ». Il avait utilisé son cybercafé, le Silicon Valley Internet Coffee, à Nanchong, pour faire circuler des articles qui critiquaient les autorités et pour publier des articles prodémocratiques dans un groupe de discussion Internet. Il a été accusé d'« incitation à renverser l'État ». Il n'a pas encore comparu devant les tribunaux.

> Le 19 septembre 2000, Qi Yanchen, rédacteur en chef de la publication en ligne *Consultations*, était reconnu coupable de « subversion » et « d'avoir fait circuler de l'information antigouvernementale sur Internet » et condamné à quatre ans de prison. Le Bureau de la Sécurité publique (BSP) prétend qu'il a utilisé le pseudonyme Ji Li pour écrire des articles pour le mensuel *Kaifang* de Hong Kong et le bulletin dissident *VIP Reference*. Il aurait aussi publié des extraits de son livre *The Fall of China*, qui appelle à une réforme politique. La police a confisqué son ordinateur, son télécopieur et ses notes.

> Le 13 mai 2000, le gouvernement suspendait les activités du site China Finance Information Network pour deux semaines et condamnait ses propriétaires à une amende. La publication financière en ligne était accusée d'avoir fait courir « des rumeurs qui pouvaient ternir l'image du gouvernement » après la publication d'un article sur la corruption d'un responsable politique régional.

> Le 3 août 2000, les responsables de la sécurité débranchaient et interdisaient le site www.xinwenming.net pour avoir fait circuler de « l'information contre-révolutionnaire » et attiré « une grande partie de la communauté dissidente de Chine ». Les cinq dissidents responsables du site sont actuellement recherchés par la police mais n'ont pas encore été arrêtés. Créé le 29 avril 2000, www.xinwenming.net est le premier site hébergé en Chine qui invitait ouvertement à la « réconciliation nationale et à la démocratie ».

Transfert des technologies et convergence des politiques

Le droit à la liberté d'opinion, d'expression et d'information
Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.

Article 19 de la Déclaration universelle des droits de l'homme

La mondialisation affaiblit le contrôle national de la circulation des données. Le développement d'Internet est peut-être le meilleur exemple d'une technologie mondiale. La combinaison mondialisation et convergence numérique a dans plusieurs pays en développement un effet dévastateur sur la vie privée. Dans le domaine des technologies de l'information et des communications, la vitesse de la convergence des politiques augmente tellement rapidement que même les pays les plus développés doivent forcer l'allure pour rattraper les progrès de la technologie. Dans la sphère de la surveillance numérique – écoute en ligne, systèmes d'identification personnelle, exploration de données, censure ou chiffrement –, ce sont invariablement les pays industrialisés qui établissent les règles du jeu pour le reste du monde.

Fait de plus en plus inquiétant, cette technologie de surveillance est exportée, sans se préoccuper des fins de l'acquéreur, vers des pays qui violent de manière flagrante les droits humains fondamentaux de leurs citoyens. Les gouvernements des pays dont les infrastructures sont sous-développées comptent sur les pays industrialisés pour leur fournir de l'équipement de surveillance. Le transfert des technologies de surveillance d'un pays développé à un pays en voie de développement est devenu un composant important de l'industrie de l'armement de l'après-guerre froide.[8] La normalisation transfrontalière, avec le peu d'attention qu'elle prête aux variations dans le respect des droits humains, porte plusieurs à croire qu'une architecture mondiale de surveillance électronique est en train de naître et que celle-ci émane des responsables de l'application des lois aux États-Unis.

Opération Root Canal

Dès 1988, dans le cadre d'un programme surnommé « Operation Root Canal »[9] au sein du Federal Bureau of Investigation (FBI) des États-Unis, les fonctionnaires chargés de l'application des lois dans ce pays demandaient aux compagnies de téléphone de modifier leur équipement pour faciliter l'interception des appels. Toutes les grandes entreprises internationales de télécommunications, à l'exception d'une seule, ont refusé de se plier à cette demande. L'exception était Nortel Networks, une entreprise canadienne, qui a accepté de travailler en collaboration étroite avec le FBI.[10] Plus de 75 % du trafic principal Internet nord-américain passe par les systèmes de Nortel et un important pourcentage des revenus de cette dernière provient du marché des télécommunications des États-Unis.

Après plusieurs années de lobbying par le FBI, le Congrès des États-Unis a adopté en 1994 la Communications Assistance for Law Enforcement Act (CALEA).[11] La CALEA oblige les transporteurs terrestres et cellulaires ainsi que les fabricants d'équipement de télécommunications à s'assurer que tout leur équipement, toutes leurs installations et tous leurs services permettent au gouvernement d'intercepter toute communication, filaire ou non, transmise par le télécommunicateur au moment de sa transmission.[13] Les communications doivent s'effectuer de manière à pouvoir être transmises à une installation distante du gouvernement.[14]

L'adoption de la CALEA fut controversée, le FBI cherchant continuellement à amender le projet de loi pour y inclure des règlements de plus en plus astreignants, comme ceux en vertu desquels les téléphones cellulaires doivent permettre le repérage de l'emplacement sur demande et les compagnies de téléphone doivent fournir l'équipement nécessaire pour jusqu'à 50 000 écoutes en ligne simultanées.[15]

Le FBI faisait pression non seulement sur le Congrès et sur les compagnies aux États-Unis pour l'adoption de la CALEA, mais aussi sur les alliés des États-Unis pour que la loi devienne une norme internationale. Le FBI a d'abord sollicité les ministres de la Justice et de l'Intérieur des pays de l'Union européenne (UE) pour la création de normes techniques internationales sur l'écoute électronique.[16] En 1991, le FBI a tenu une série de réunions secrètes avec les pays membres de l'UE pour les persuader d'intégrer la CALEA aux lois européennes. En 1993, le FBI organisa, à son laboratoire de recherche de Quantico en Virginie, des séminaires consacrés au développement de standards internationaux en matière d'interception des télécommunications, baptisés International Law Enforcement Telecommunications Seminars (ILETS). Des représentants du Canada, de Hong Kong, de l'Australie et de l'Union européenne y participèrent. Résultat : l'adoption d'une norme technique internationale de surveillance, la « International Requirements for Interception ».[17]

Selon un rapport de l'UE,[18] la stratégie prévoyait que les pays industrialisés s'entendent sur des normes et des procédures puis qu'ils vendent leurs produits aux pays en voie de développement. Même si les pays industrialisés refusaient de se plier aux ordres d'interception, les communications sont quand même surveillées par le réseau Signals Intelligence UK-USA « dès qu'ils utilisent l'équipement ».[19] Les efforts du FBI furent récompensés : en janvier 1995, le Conseil des ministres de l'UE adoptait discrètement une résolution dont le texte est presque mot pour mot celui des exigences nationales du FBI.[20] La résolution ne fit l'objet d'aucun débat officiel et n'a été rendue publique qu'à la fin de 1996.

Les ILETS se poursuivirent. Des comités furent mis sur pied pour élaborer une norme plus détaillée dans le but d'étendre la portée des standards d'interception. La nouvelle norme devait s'appliquer à un grand éventail de technologies des communications, notamment Internet et les communications par satellite, et établir des exigences plus détaillées relatives à la surveillance de toutes les technologies. Résultat : un document de 42 pages, ENFOPOL 98 (la désignation de l'Union européenne pour les documents produits par le Groupe de travail sur la coopération policière de l'Union).[21]

En 1998, le document est rendu public et soulève beaucoup de critiques. Les comités réagissent en produisant un nouveau document, ENFOPOL 19, expurgé de la plupart des détails controversés, mais qui en revanche étend le type de surveillance pour y inclure les adresses IP, les numéros de cartes de crédit et les adresses de courrier électronique.[22] En avril 1999, le Conseil propose la nouvelle ébauche d'une résolution en faveur de l'adoption des normes ENFOPOL 19 dans les lois de l'Union européenne.

En mai 1999, le Parlement européen approuve la résolution ENFOPOL 19. Le vote a lieu un vendredi soir en présence de 20 % seulement des délégués et est ensuite renversé par le Conseil des ministres. Ce rejet n'a pas empêché l'Institut européen pour les normes de télécommunications (ETSI) de poursuivre son travail d'élaboration de normes internationales sur l'écoute en ligne.

Que voulez-vous que soit Internet ?

« Un contact humain. Je veux qu'il sache qui je suis. »[23]

Au salon tenu à Beijing en novembre 2000, les plus grands noms en technologie Web – des entreprises qui s'associent fièrement outre-mer à la réputation anarchiste d'Internet[24] – tentaient de vendre leur marchandise à la police secrète et aux fonctionnaires de la sécurité de la Chine. Qualifié de « plus grande exposition de sécurité nationale », le salon Security China 2000 était le deuxième événement de ce genre commandité par le ministère de la Sécurité publique (MPS) en autant d'années. Parmi les organisateurs, la « Chinese Communist Party Central Committee's Commission for the Comprehensive Management of Social Security »[25] (Commission sur la gestion de la sécurité publique du Comité central du Parti communiste de Chine) est responsable de l'appareil de sécurité de l'État dans son ensemble, du contrôle des travailleurs itinérants et des campagnes anticrimes jusqu'à la surveillance des activités des dissidents.

Le *Shanghai Business Magazine* a récemment évalué à 15 % la croissance annuelle de l'industrie chinoise de la sécurité. Outre-mer, les spécialistes ont prédit dans le journal *Security World* une croissance de 20 % au cours des trois à cinq prochaines années. On s'attend à ce que, dans les dix prochaines années, la Chine devienne le deuxième marché de sécurité au monde, précédé des États-Unis.[26]

Le salon, organisé par la société Adsale Exhibition Services Ltd. de Hong Kong, a attiré environ 300 entreprises de plus de 16 pays de même que 24 500 visiteurs de plus de 26 provinces de Chine. Parmi les invités spéciaux : Jia Chunwang, ministre de la Sécurité publique. Selon Adsale, le salon Security China 2000, comparativement à celui de 1998, affichait une augmentation de 50 % du nombre d'exposants internationaux et de 80 % de la surface d'exposition.[27] Les géants de l'industrie des réseaux s'y côtoyaient : Siemens, Motorola, Cisco Systems, Sun Microsystems et Nortel Networks, entourés d'entreprises des États-Unis, d'Israël, de France, d'Allemagne, des Pays-Bas, du Japon et du Canada, parmi d'autres. Le Royaume-Uni, chef de file mondial en télévision en circuit fermé, occupait une section spéciale.

Le projet Bouclier d'or

Au salon Security China 2000, le nouveau projet Bouclier d'or du ministère de la Sécurité publique a rapidement ravi la vedette. Son but : promouvoir l'adoption de technologies de l'information et des communications évoluées pour renforcer le contrôle policier central, améliorer les capacités de réaction, aider à mieux combattre le crime et rendre plus efficace le travail des policiers.[28] L'appareil de sécurité de la Chine a de grandes ambitions : construire un réseau de surveillance numérique à l'échelle de la nation, permettant de relier les agences de sécurité locales, régionales et nationales dans un circuit de surveillance globale. Beijing voit le projet Bouclier d'or comme un système de télésurveillance fonctionnant à partir de bases de données avec accès immédiat aux dossiers d'enregistrement de chaque citoyen et des liens vers de vastes réseaux de caméras visant à améliorer le temps de réponse de la police lors de manifestations.

Même si le projet n'en est qu'à ses débuts, les chefs de l'industrie chinoise présents au salon ont évalué que le gouvernement avait dépensé 600 millions RMB (70 millions de dollars US) en recherche et que le total des dépenses s'élèverait à maintes fois ce montant.

Le projet Bouclier d'or, selon l'information disponible sur le site Web du salon, porte principalement sur les secteurs suivants de la sécurité : contrôle de l'accès, systèmes anti-piratage informatique, sécurité des communications, logiciels et accessoires informatiques, chiffrement et déchiffrement, sécurité du commerce électronique, sécurité d'Internet et des intranets, dispositifs coupe-feu, communications réseau, sécurité et gestion de réseau, sécurité des transactions, sécurité des cartes intelligentes, sécurité des systèmes, détection de virus, services TI et autres.[29]

La réussite du projet Bouclier d'or repose sur un grand éventail de technologies évoluées. Bien que la recherche technologique en Chine ait fait des pas de géant dans ces secteurs et dans d'autres domaines, les scientifiques chinois n'ont développé aucun des composants nécessaires à la réalisation du projet Bouclier d'or de manière autonome. Ils ont toujours été appuyés par les entreprises occidentales, qui leur vendent des solutions clés en main ou qui leur transfèrent la technologie au moyen d'ententes commerciales officielles ou souvent en contrepartie d'un accès plus grand au marché.

Les technologies nécessaires pour supporter un réseau intelligent de surveillance de masse sont d'une complexité affolante. Toutefois, puisque les solutions ont pour modèle les formes humaines d'intelligence, on peut, pour en parler, utiliser des termes qui nous sont familiers. Le réseau de surveillance Bouclier d'or de Beijing doit « voir », « entendre » et « penser ».

La technologie qui permet au réseau d'« entendre » – par exemple de surveiller automatiquement les conversations téléphoniques, à la recherche de mots et de phrases clés – repose sur le traitement des signaux de conversation. Pour sa part, le traitement des signaux vidéo permet au réseau, par le biais de caméras de surveillance, de « voir » – par exemple de reconnaître des visages dans une foule. Ces deux « sens », deux types de traitement numérique des signaux (DSP), sont appelés « systèmes algorithmiques de surveillance » parce qu'ils analysent les données au moyen d'algorithmes complexes modelés sur le système nerveux humain. Dans le traitement des signaux de conversation par exemple, la cochlée pourrait servir de base pour l'abstraction mathématique.

En Chine, le chef de file dans ce domaine est le Département d'ingénierie électronique de la prestigieuse Université de Tsinghua. Une équipe de recherche de ce département travaille sur la reconnaissance de la parole depuis le début des années 80. Cette recherche est financée par le gouvernement de Chine et par Nortel Networks (de 1995 à 1998)[30] et menée en parallèle avec celle de Nortel sur la reconnaissance de la parole, en collaboration avec le FBI.

Les fonds du gouvernement de Chine alloués au projet de reconnaissance de la parole proviennent des budgets nationaux alloués aux projets 863 sur la technologie de pointe.[31] Un projet 863 a débuté en mars 1986, en réaction au projet de défense stratégique « Guerre des étoiles » de l'administration Reagan.[32] Ce projet 863 accorde les investissements du gouvernement en priorité à sept volets distincts qui comportent des applications militaires et de sécurité de l'État, dont la technologie de l'information, et les systèmes à laser et antisatellites. Certains projets 863 sont supervisés par l'agence chinoise de développement de l'armement (Chinese Weapons Development Agency).[33]

À la fin de 1998, les ingénieurs de Tsinghua annonçaient qu'ils mettaient au point un grand système de reconnaissance de la parole continue à vocabulaire étendu indépendante du locuteur sur voie téléphonique. Ce système en temps réel est utilisé par les dispositifs téléphoniques et les systèmes de service d'information sur des liaisons téléphoniques, avec un taux de reconnaissance de plus de 98 %.[34] Ces ingénieurs prétendaient orienter la recherche vers la reconnaissance de la parole continue à vocabulaire étendu (voire illimité) indépendante du locuteur et la reconnaissance de la parole à vocabulaire étendu téléphonique pour mettre au point une technologie qui s'adapte rapidement à la voix du locuteur afin d'améliorer l'exactitude de la reconnaissance de la parole indépendante du locuteur.[35] Cette recherche est parallèle au développement de la technologie nécessaire à l'application de la CALEA aux États-Unis. En d'autres mots, il semble que cette recherche n'a pas d'autre but que la surveillance automatique des communications téléphoniques.

Une alliance inconvenante

Le département d'ingénierie de Tsinghua entretient des relations étroites avec le laboratoire de Recherches Bell-Northern (BNR) à Montréal, une filiale de recherche et développement de Nortel,[36] où fut mis au point le module de reconnaissance de la parole de Nortel. Au cours de sa mission commerciale en 1998, le premier ministre Jean Chrétien a annoncé que Nortel Networks et Tsinghua établiraient un laboratoire de recherche commun.[37] Un des objectifs premiers du laboratoire de recherche était d'augmenter l'expertise en réseau de la Chine. L'entente comprenait également un « programme d'échange d'experts » entre Nortel Networks et l'Université Tsinghua pour une meilleure collaboration. En effet, des diplômés du département d'ingénierie de Tsinghua ont joué des rôles déterminants dans la mise au point du module de reconnaissance de la parole de Nortel.

Encadré 2 :

Les projets « Golden » de la Chine : « Modernisation » de l'économie de la Chine

Les projets Golden étaient des initiatives de la Chine dans les domaines des télécommunications et des infrastructures d'information dans les années 90. Ils étaient répartis en quatre phases :

La phase I regroupait quatre projets : **Golden Bridge** – l'infrastructure du réseau d'information économique national de la Chine ; **Golden Gate** (douanes) – un réseau d'information sur le commerce extérieur raccordant le ministère du Commerce extérieur et de la Coopération économique au Bureau des douanes ; **Golden Card** – un projet expérimental sur l'argent électronique ; et **Golden Sea** – un système d'information reliant les chefs du gouvernement de la Chine et leur permettant d'accéder aux données de toutes les institutions et organisations et de tous les bureaux soumis à la juridiction directe du Comité central du Parti communiste.

La phase II visait à mettre les réseaux d'information au service de la réforme économique. **Golden Macro** – le groupe financier et économique central du gouvernement pour un macro-contrôle des activités économiques nationales ; **Golden Tax** – un réseau de données reliant le centre de vérification de l'administration fiscale de l'État à Beijing à 50 bureaux régionaux et 800 centres de service ; et **Golden Intelligence** – le service Internet de la Chine.

La phase III se rapportait aux applications sectorielles du nouveau programme TI. **Golden Enterprise** – la construction d'intranets dans 12 000 grandes et moyennes entreprises de Chine et leur interconnexion en fonction des différents cercles d'affaires ; **Golden Agriculture** – un réseau de banques de données pouvant fournir de l'information sur l'agriculture, des rapports météorologiques et de l'information sur les marchés ; **Golden Health** – le système d'échange d'information du ministère de la Santé publique pour les hôpitaux ; **Golden Information** – un réseau reliant divers services de collecte de statistiques en Chine ; et **Golden Housing** – une base de données de renseignements sur le secteur immobilier à l'échelle nationale.

La phase IV comprenait le projet **Golden Cellular** – un consortium national des plus grands fabricants d'équipement de communications mobiles en Chine ; et **Golden Switch** – un programme pour la construction d'une industrie nationale de fabrication d'autocommutateurs numériques en Chine.

Tsinghua a établi des statistiques sur les formes phraséologiques courantes utilisées pendant un appel téléphonique. Deux cent quatorze formes de différentes commandes ont été dénombrées. Tsinghua a mis au point la plus grande base de données sur la parole en Chine.[38]

Étant donné l'engagement précoce de Nortel dans l'élaboration de normes appuyant la CALEA, il est bien normal que le premier autocommutateur numérique à être offert sur le marché et à offrir aux fournisseurs de services la possibilité de se conformer à la CALEA soit fabriqué par Nortel.[39]

Les commutateurs DMS Supernode sont fabriqués en Chine, le résultat d'une coentreprise avec le gouvernement chinois, la GDNT (Guangdong Nortel). Nortel affirmait à l'époque que ce transfert de technologie contribuerait énormément au développement de l'industrie des télécommunications en Chine.[40]

Nortel a investi 37 millions de dollars supplémentaires dans la GDNT (cette somme s'ajoutant au financement accordé selon le protocole d'entente de 1993 avec la commission de planification de l'État) – un investissement qui emboîtait le pas à l'annonce du gouvernement des États-Unis de compenser les fabricants d'équipement pour l'application de la CALEA.[41]

Au-delà de la grande muraille électronique : de la censure à la surveillance

Le rythme et l'ampleur du développement du réseau Internet en Chine ont réduit l'importance de la « grande muraille électronique » constituée de passerelles reliées à un intranet national sécurisé. L'idée de départ d'établir un intranet à l'échelle de la Chine a été dépassée par les événements, plus particulièrement par la libéralisation du secteur des télécommunications de la Chine.

Malgré la politique officielle d'ouverture que suggère l'entrée prochaine de la Chine dans l'Organisation mondiale du commerce, certains fonctionnaires chérissent toujours l'idée d'un réseau d'information chinois isolé des dangereuses tentations du WWW. « La Chine doit bâtir un réseau national indépendant d'Internet », a déclaré Jiang Mianheng, fils de Jiang Zemin et vice-président de l'Académie chinoise des sciences, au cours d'une conférence à Shanghai en juin dernier.[42]

Par contre, le concept des passerelles a survécu, bien qu'en partie ébranlé par des facteurs financiers et techniques. Le nombre de raccordements et le débit de transmission ont augmenté en réponse à la demande croissante des entreprises et des utilisateurs. En effet, la vitesse passait de 84,64 Mbit/s (été 1998) à plus de 351 Mbit/s (fin de 1999) et à plus de 2,5 Gbit/s (2001). Les exigences de sécurité et de contrôle ont cédé à la demande économique pour des réseaux à convergence large bande.

Les implications de la mise en place de dispositifs coupe-feu pour empêcher les Chinois d'accéder à du matériel interdit sur des sites à l'extérieur du pays sont bien connues. Bon nombre des technologies utilisées pour la sécurité informatique peuvent servir à restreindre les droits humains et la démocratie au moyen de l'intimidation et de la surveillance systématique de la population.

Le ministère de la Sécurité publique a annoncé l'an dernier que d'ici trois ans il aura créé une base de données nationale contenant les renseignements personnels et les numéros d'identification de chaque adulte au pays. Le gouvernement chinois a toujours maintenu un fichier cumulatif (appelé *dangan*) sur la performance et les attitudes de chaque personne à partir de la maternelle jusque sur le marché du travail. Cette information sera numérisée et chaque Chinois recevra une nouvelle carte d'identification de deuxième génération dotée d'une micropuce contenant son *dangan*. Actuellement, la carte d'identification est en papier laminé avec photo, et indique le nom de la personne, sa date de naissance et son numéro d'identification. Cette carte papier « est relativement facile à contrefaire », a récemment affirmé Qiu Xuexin, le directeur du plus important institut de recherche soumis à la juridiction du Bureau de la Sécurité publique,[43] à la quatrième foire internationale de la carte intelligente (Fourth International Fair of Smart Cards). Qiu a ajouté que, grâce aux techniques évoluées de chiffrement, il sera plus difficile aux personnes non autorisées à le faire d'accéder aux renseignements du gouvernement contenus dans la nouvelle carte. La seconde génération de carte intelligente sera fort probablement une « carte de proximité », c'est-à-dire qu'elle pourra être balayée instantanément à une distance de plusieurs pieds et à l'insu du porteur.[44]

En mai dernier, le ministère de la Sécurité publique (MSP) a installé chez les fournisseurs de services Internet deux boîtes noires – des dispositifs de surveillance destinés à surveiller le contenu et les activités des comptes de courrier électronique. En outre, les autorités travaillent avec des experts en technologie de l'Université Shenzhen à la mise au point d'un « système de filtrage des courriers électroniques » capable de déceler les messages « indésirables » à l'insu

du destinataire ou du moins sans son consentement.[45] Tout récemment, le MSP a participé à la création de faux serveurs mandataires pour surveiller les navigateurs qui tentent de contourner les coupe-feu officiels.[46]

Comme en 1998, Security China 2000 a été tenu en même temps que son événement frère, Building China 2000. Le projet Bouclier d'or prévoit la construction d'immeubles intelligents et certains fournisseurs font la promotion de leurs systèmes aux deux salons. Datang Telecom, une entreprise chinoise récemment impliquée dans un cas d'espionnage industriel contre Lucent, annonçait, à la suite de ces deux expositions, qu'elle avait décroché un contrat de construction d'un immeuble intelligent pour le Bureau de la Sécurité publique provincial de Jilin.

En vertu du contrat, Datang Telecom doit assurer la conception et l'implantation du projet en accomplissant toutes les tâches, notamment l'installation du système de surveillance, du câblage intégré et des réseaux informatiques. L'implantation de ce projet concrétise et rend plus visible le projet Bouclier d'or qui sera bientôt réalisé dans le secteur de la sécurité publique nationale.[47]

Sur un site Web consacré à la promotion du projet Bouclier d'or, le MSP annonçait récemment d'autres plans semblables sur l'intégration des réseaux de surveillance CCTV (télévision en circuit fermé) dans l'environnement urbain à Guangdon.[48]

Datang a également mis au point son propre logiciel de filtrage du courrier électronique et un certain nombre de coupe-feu. Elle jouit de relations privilégiées avec des fabricants outre-mer d'équipement de télécommunication, entre autres pour des projets conjoints de recherche et de transfert des technologies. Datang a bénéficié par exemple d'un projet de recherche conjoint avec Nortel portant sur le protocole sans fil CDMA, à partir duquel elle a mis au point la version chinoise du protocole : TD-SCDMA.

Bien que la Chine ait incontestablement ses propres programmes de recherche évoluée et qu'elle mette au point ses propres systèmes de sécurité, elle s'appuie essentiellement sur l'expertise fournie par des entreprises transnationales et des partenariats, sur le transfert de technologie et sur des investissements directs, et ce, même pour la technologie de base.

Bien sûr, les entreprises ne se vantent pas de telles relations. Motorola, par exemple, fournit des dispositifs de communication sans fil à la police chinoise responsable de la surveillance de la circulation routière. Or, des journalistes ont raconté qu'au salon Security China 2000, ses représentants ont refusé de répondre à leurs questions sur la participation de Motorola au projet Bouclier d'or. Orin Li, de Compaq China, est resté tout aussi évasif, en affirmant que son entreprise « n'était pas la seule », que « tout le monde le faisait » et en encourageant le journaliste à aller interroger la compagnie Sun.[49]

Sun Microsystems est certainement engagée dans le transfert de haute technologie à l'appareil de sécurité de la Chine. Elle a mis au point, en collaboration avec Hongda Group de Changchun, chef de file en technologie de reconnaissance des empreintes digitales, un réseau informatique reliant les 33 commissariats de police provinciaux, formant ainsi la couche du projet Bouclier d'or qui permet au Bureau de la Sécurité publique de comparer instantanément des empreintes digitales avec une base de données nationale.

Fournisseur d'un grand nombre de routeurs et de dispositifs coupe-feu au réseau de Chine, Cisco Systems est un autre exemple. Au salon Security China 2000, une représentante de ce géant en réseaux informatiques a affirmé au groupe de fonctionnaires du Bureau de la Sécurité publique que Cisco était le chef de file mondial en coupe-feu et que la Chine constituait un énorme marché potentiel pour ce type de technologie.[50]

Internet et la vie privée

Le droit à la vie privée

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Article 12 de la Déclaration universelle des droits de l'homme

Un des défis que doit relever l'appareil de sécurité de la Chine en conséquence du déclin de l'efficacité de la « grande muraille électronique » est de passer de dispositifs coupe-feu qui filtrent le contenu à l'échelle nationale à un filtrage au niveau des habitations et des bureaux, soit la redistribution de la grande muraille électronique, de cinq passerelles internationales à des millions d'ordinateurs personnels et de cellulaires.

L'impact de cette stratégie est énorme sur la vie privée des utilisateurs puisque la surveillance des citoyens par le gouvernement devient une réalité et qu'elle fait appel à des technologies qui restreignent fortement la liberté d'expression des utilisateurs chinois d'Internet. Il devient beaucoup plus difficile pour les activistes défenseurs des droits humains et de la démocratie de communiquer à l'insu du gouvernement avec des sources d'information « illégales ».

Cette tendance, c'est-à-dire ce déplacement d'un contrôle du contenu généralisé au niveau d'une passerelle vers une surveillance des utilisateurs aux extrémités du réseau, est facilitée par les nouvelles technologies de gestion du contenu transmis sur large bande.

Au salon Security China 2000, Nortel Networks vantait au ministère de la Sécurité publique son réseau de surveillance numérique JungleMUX et sa gamme de produits OPTera Metro. JungleMUX est un système d'avant-garde de transport des images vidéo d'un réseau de télésurveillance à un centre de contrôle. Les produits OPTera Metro sont le point d'appui de l'initiative « Internet Personnel » de Nortel. Ils permettent aux fournisseurs de services Internet de mieux surveiller les utilisateurs d'Internet et leurs activités en ligne. Les défenseurs du droit à la vie privée aux États-Unis ont fortement dénoncé cette pratique.[52]

La présentation de Nortel au salon Security China 2000 a sûrement fait de l'effet. Shanghai Telecom (ST) a récemment annoncé qu'elle avait choisi les produits OPTera de Nortel pour son futur réseau optique large bande urbain de la prochaine génération. Que signifie ce contrat, évalué à plus de 10 millions de dollars US ? Que Nortel construira le premier réseau optique urbain en Chine et qu'elle fournira un système d'accès large bande et une solution ADSL qui assureront le service numérique haute vitesse à environ 200 000 abonnés. Le projet devrait être terminé à temps pour assurer les services Internet et de vidéoconférence à la réunion des chefs d'État de l'APEC prévue à Shanghai en octobre 2001. Shanghai, principale animatrice de la nouvelle économie chinoise, pourra se vanter de posséder un des réseaux urbains les plus évolués au monde.

Grâce aux produits OPTera, au cœur de la stratégie « Internet Personnel » de Nortel, Shanghai Telecom a pu construire un réseau optique parallèle évolué pouvant prendre en charge la diffusion multimédia en temps réel et autres transactions sensibles aux délais. Il est très difficile d'obtenir la diffusion multimédia en temps réel sur des circuits Internet ordinaires. Bien que les liaisons optiques d'avant-garde de Nortel permettent d'augmenter radicalement

la largeur de bande disponible à la ville de Shanghai, ce n'est pas ce qui intéresse ceux qui cherchent à protéger le réseau de Chine contre de nouvelles menaces de plus en plus sophistiquées. Les produits OPTera d'intérêt certain sont ceux sur lesquels repose la stratégie Internet Personnel : Shasta et Alteon,[53] de Nortel. Grâce à ceux-ci, Shanghai Telecom (ST) pourra offrir des services Web personnalisés aux entreprises et aux consommateurs, c'est-à-dire personnaliser les services de livraison du contenu au moyen d'un réseau conscient du contenu et de l'utilisateur. Le réseau peut « penser », soit identifier les abonnés lorsqu'ils entrent en communication, faire correspondre des noms à des adresses IP et apprendre à connaître les goûts des abonnés en matière de contenu.

Le Shasta 5000 BSN alimente l'extrémité abonné du réseau, là où les technologies « locales », comme la DSL de haute qualité, sont raccordées au réseau principal Internet et là où les abonnés accèdent aux services et au contenu large bande. Shasta est un point de regroupement universel où accès commuté, DSL, connexions filaires et sans fil, liaisons relais de trames/technologie ATM et lignes privées se raccordent à Internet. Pour ST, l'avantage concurrentiel que procure Shasta est un réseau de services large bande à valeur ajoutée. En raison du nombre de caractéristiques de sécurité qu'il recèle, Shasta constitue également un avantage pour le Bureau de la Sécurité publique de Shanghai, le plus évolué des services policiers en ligne de la Chine.

« Imaginez un réseau qui sache qui vous êtes, où vous êtes et qui puisse vous joindre sur votre cellulaire tout comme sur votre ordinateur. Mieux, imaginez qu'au lieu de trouver votre contenu Web, ce soit vous qu'il trouve. Une affaire personnelle. Exactement. »[51]

– Nortel Networks, Stratégie Internet Personnel

La stratégie Internet Personnel est présentée à ST comme elle l'est en Occident, c'est-à-dire comme un moyen d'augmenter les profits générés par les réseaux en offrant entre autres des services de sécurité ou en permettant la revente de données à d'autres entreprises. Cette pratique de revente de données personnelles, condamnée par les défenseurs du droit à la vie privée, est formellement exclue dans la déclaration de confidentialité de Nortel. Pourtant, la stratégie Internet Personnel repose sur la capacité du réseau à faire correspondre des adresses IP aux profils démographiques des utilisateurs.

Nortel présente sa stratégie Internet Personnel comme la clé du futur d'Internet. C'est pourquoi cette stratégie occupe le centre de sa dernière campagne de publicité. Il est tout à fait remarquable que Nortel puisse promouvoir auprès d'autres entreprises des pratiques commerciales qu'elle affirme exclure de ses propres activités.

Grâce à Internet Personnel de Nortel, le Bureau de la Sécurité publique de Shanghai peut faire bien plus que simplement surveiller les accès au Web en ciblant certains auditoires et en créant des profils démographiques en temps réel. Un tel système de distribution et de livraison sur réseau intelligent a un impact formidable sur la vie privée des utilisateurs. Internet Personnel est un réseau qui sait toujours « qui vous êtes ».

Les utilisateurs qui accèdent au réseau au moyen de diverses technologies d'accès comme la DSL, l'accès par câble ou l'accès sans fil reçoivent des paramètres de sécurité qui sont appliqués par abonné. Doté d'une capacité extraordinaire de traitement de paquets, Shasta est l'une des plus puissantes plates-formes de classe transporteur pour la gestion de la sécurité réseau. Le service large bande de marché de masse et la connectivité permanente entraînent de nouvelles inquiétudes sur le plan de la sécurité. Le Shasta 5000 BSN offre des

fonctions étendues de coupe-feu faciles à fournir et permettant la surveillance en permanence du flux de transmission de chaque individu.

L'accès large bande contraste avec l'accès commuté classique en vertu duquel les abonnés communiquent avec leur fournisseur de services Internet (FSI), font leur petite affaire puis coupent la communication. La nature brève de l'accès commuté n'offre guère le temps d'exploiter un point faible de la sécurité. Par conséquent, les incidents de sécurité au moyen de l'accès commuté sont peu nombreux et sans grande envergure.

« Nortel Networks s'engage à ne pas vendre, louer ni divulguer ces informations auprès d'autres organisations. »[54]

« Nortel Networks collecte les adresses IP pour l'administration du système et le suivi interne. Lorsque vous visitez notre site, nos serveurs consignent seulement les adresses IP. Nous ne lions pas les adresses IP à des informations personnellement identifiables. »[55]

– Déclaration de confidentialité de Nortel, 2000

Les entreprises disposant de liaisons d'accès spécialisées (T-1, relais de trames) sont protégées. Mais, en raison du coût élevé de ces liaisons, les petites et moyennes entreprises, les consommateurs, les groupes d'intérêt et les organismes non gouvernementaux hésitent à y avoir recours. Ils utilisent des accès large bande qui sont raccordés en permanence à Internet. Pourtant, actuellement, la plupart des utilisateurs de la DSL ou du câble sont raccordés à Internet sans coupe-feu et sont par conséquent très vulnérables. Cette question constitue une vraie menace pour la sécurité des réseaux.

L'extrémité abonné

Pour contrer cette menace, Shasta de Nortel offre une couche de sécurité qui se positionne entre les coupe-feu personnels et des solutions d'entreprise bien plus coûteuses. Ce produit intègre une fonction évoluée de coupe-feu basée sur des politiques et sur des états, avec authentification à distance, enregistrement des activités, chiffrement et filtrage du contenu. Shasta étant situé à l'extrémité du réseau, le fournisseur de services peut appliquer ses politiques de sécurité à chaque abonné au moyen d'une interface au lieu de laisser aux abonnés le soin de gérer la sécurité.

L'« extrémité abonné » est le point de regroupement dans le réseau du fournisseur de services, soit le point de contact entre l'abonné et le réseau. Il s'agit du seul point dans le réseau où le fournisseur de services peut « voir » l'abonné et contrôler les flux de données. Au-delà de ce point, le trafic de plusieurs abonnés est regroupé sur des connexions haute vitesse et acheminé vers des routeurs principaux. Lorsque le trafic parvient à la passerelle internationale, il est impossible pour les agences de surveillance de distinguer les flux individuels de trafic.

La solution de sécurité de Nortel repose sur le principe suivant : le seul point viable dans le réseau où le fournisseur de services peut appliquer quelque forme de contrôle que ce soit sur le trafic d'un abonné est à l'extrémité abonné. En d'autres mots, même si le logiciel de sécurité est situé dans le PC de l'abonné, il est géré à distance par son FSI. Cette stratégie marque la fin de la « grande muraille électronique », puisque la surveillance et le contrôle du contenu

s'effectuent maintenant sur le trafic à l'extrémité du réseau plutôt qu'en son centre, c'est-à-dire au niveau d'une passerelle internationale.

Une autre fonction de sécurité importante de Shasta : une technologie évoluée qui empêche la contrefaçon d'adresses IP. La contrefaçon informatique consiste à envoyer du trafic à partir d'une adresse IP apparemment autorisée et par conséquent acceptable par le coupe-feu, alors qu'il s'agit en fait d'une adresse dont s'est emparé le pirate pour une utilisation illégale. Même les coupe-feu les plus évolués peuvent être trompés par un bon pirate. Le Shasta 5000 BSN peut empêcher les pirates d'accéder au réseau d'un abonné parce qu'il applique des fonctions anticontrefaçon au niveau de chaque abonné. Le coupe-feu Shasta 5000 BSN peut filtrer le trafic en provenance ou à destination d'un abonné et empêcher l'utilisateur final de produire des paquets contrefaits ou de transférer le trafic d'un autre abonné.

Les répercussions sont multiples. Tandis que le produit améliore la protection contre les attaques de type interruption de service, il présente tout un défi aux systèmes créés pour aider ceux qui tentent de contourner les coupe-feu de la Chine, notamment les dissidents et les activistes en faveur de la démocratie.

Une ombre virtuelle

Les fournisseurs de services procèdent à la vérification de l'identité pour valider l'accès des utilisateurs à leurs réseaux. Les mécanismes d'authentification sont nombreux : nom d'utilisateur et mot de passe, cartes intelligentes, dispositifs biométriques tels que les balayeurs d'empreintes digitales et les systèmes de reconnaissance des visages.

Le Shasta 5000 BSN permet plusieurs types d'authentification des utilisateurs, en fonction du mécanisme et du protocole d'accès. Par exemple, pour l'accès d'un administrateur au Shasta 5000 BSN, l'authentification s'effectue actuellement au moyen d'un mot de passe, mais l'authentification biométrique n'est pas exclue.

L'enregistrement des activités permet d'effectuer un suivi des activités au sein du réseau et à son extrémité pour déterminer si le trafic rejeté constitue une menace ou respecte un plan ordonné. Ces renseignements peuvent ensuite servir à améliorer les fonctions de sécurité du réseau et à justifier la surveillance d'utilisateurs « illégaux ».

Le Shasta 5000 BSN fournit une interface utilisateur graphique (IUG) pour la création et la définition de l'enregistrement de toutes les activités ainsi qu'un gestionnaire de journal qui affiche chaque événement enregistré par abonné et par service. L'information du journal est stockée puis acheminée vers des bases de données distantes. Tous les événements, incluant l'acceptation ou le rejet de paquets, peuvent être enregistrés dans un journal en fonction de

critères système et sont horodatés au moment où ils se produisent. Tous les paquets abandonnés en raison de leur non-conformité à un comportement « normal » de protocole peuvent également être enregistrés dans le gestionnaire de journal à des fins d'analyse.

Le gestionnaire de journal de Shasta permet l'analyse, le filtrage et la recherche dans le journal, et ce, de différentes façons, afin d'extraire rapidement et efficacement de l'information très détaillée sur les habitudes de communications d'une personne. Cette information peut ensuite être stockée dans d'énormes bases de données locales et centralisées où elle demeure disponible pour d'autres analyses par le MSP. Celui-ci peut par exemple établir des correspondances entre de « vrais » événements et des habitudes de trafic Internet. Une montée subite inhabituelle du nombre de courriels envoyés pendant la journée avant une manifestation, par exemple, produirait beaucoup de données même sans avoir accédé au contenu des messages.

Le filtrage du contenu constitue un autre moyen de contrôler le contenu Internet entrant dans n'importe quel environnement – à la maison, à l'école, au cybercafé et au bureau. Des filtres bloquent, dans une circonstance ou un environnement particulier, certaines URL qui répondent à des critères ou font partie de certaines catégories. Des centres régionaux de sécurité Internet sous le contrôle du MSP et exclusivement réservés à la maintenance de ces listes d'URL s'établissent dans toute la Chine pour faciliter, sur le plan local, l'application de la stratégie de contrôle de l'information du gouvernement.

Le filtrage est assuré au moyen de serveurs mandataires qui vérifient chaque demande Web individuelle en la comparant avec une liste d'URL interdites et en bloquant tout contenu provenant de ces URL ou qui ne répond pas aux critères du gouvernement définissant un contenu Web « sain ». Grâce à sa capacité de réacheminement vers de tels sites de serveurs de filtrage de contenu, le Shasta 5000 BSN peut prendre en charge ces services mandataires.

En effet, grâce a la fonction d'acheminement selon des politiques du Shasta 5000 BSN, le trafic d'un abonné peut être acheminé vers des serveurs de filtrage de contenu qui effectuent ce traitement pour le gouvernement.

Ce contrôle du contenu sur le plan local entraîne deux conséquences majeures pour toute personne en Chine qui tente d'accéder au contenu d'une URL de la liste « noire » du MSP. En premier lieu, il sera beaucoup plus difficile d'accéder aux sites Web proscrits puisque les fonctions de coupe-feu du Shasta sont beaucoup plus évoluées, étant situées au point de raccordement du PC de l'utilisateur à Internet. Par exemple, l'utilisation de serveurs mandataires situés à l'extérieur de la Chine, une pratique courante chez les dissidents pour contourner les coupe-feu au niveau de la passerelle, sera décelée beaucoup plus facilement et enregistrée pour donner un profil d'utilisation qui, avec le temps, paraîtra suspect.

En deuxième lieu, grâce à une gestion du filtrage de contenu au plan régional, les bureaux du MSP seront beaucoup plus impliqués dans le processus d'optimisation des données de surveillance à partir de sources de haute technologie et de leur utilisation dans des scénarios moins pointus – intégrant des données Internet à des modes classiques de surveillance du MSP comme les réseaux d'informateurs. Ce processus est impossible à gérer centralement sauf pour les cas les plus en vue, mais devient un puissant moyen de contrôle s'il est appliqué au niveau des régions, des villes et des quartiers.

Un réseau qui sait qui vous êtes et où vous êtes

Droit à la liberté d'association
Toute personne a droit à la liberté de réunion et d'association pacifiques.

Article 20 de la Déclaration universelle des droits de l'homme

Un des objectifs du projet Bouclier d'or est d'établir un réseau national de télévision en circuit fermé ou de caméras CCTV dans des endroits publics pour réduire le temps de réponse des policiers lors de manifestations.[57] Les caméras de surveillance exposées au salon Security China 2000 montraient bien la grande complexité de la nouvelle technologie. De nouveaux types de circuits permettent à la caméra d'ignorer les objets brillants qui émettent de la lumière dans son champ ; la miniaturisation rend les caméras presque invisibles ; les caméras à infrarouge assurent la surveillance dans l'obscurité.

Selon Gerrit Hurenkamp, directeur du développement à Pelco International aux États-Unis, le marché de la télévision en circuit fermé en Chine représente annuellement de 350 à 400 millions de dollars US. Un marché lucratif mais difficile à pénétrer. Les Chinois sont très éduqués et savent ce qu'ils veulent. On ne peut pas leur vendre n'importe quel produit.

Les dispositifs électroniques de surveillance vidéo de plus en plus évolués exigent une plus grande largeur de bande pour le transport des images produites à des emplacements distants vers des centres de contrôle. L'architecture du réseau doit être assez évoluée pour desservir un pays aussi étendu que la Chine et, dans la présentation de son système JungleMUX au salon Security China 2000, Nortel abordait directement cet aspect. Les signaux vidéo sur circuit fermé sont transportés dans le réseau JungleMUX de Nortel sur un réseau longue distance (WAN) à des vitesses de 1,6 à 44 Mbit/s et sont accessibles par tous les nœuds du réseau. Chaque source vidéo (caméra, magnétoscope, etc.) est numérisée au moyen d'un algorithme de compression configurable par l'utilisateur : une solution de transport CCTV efficace et évolutive.

Les modes d'enregistrement sont divers : en temps réel, de qualités diverses, et en chronocinématographie. L'enregistrement en temps réel est comme celui en télévision ordinaire (30 images par seconde, animation intégrale). La chronocinématographie est un procédé de prise de vues accélérée (quelques images par période). L'avantage de ce procédé est qu'une bande magnétique peut enregistrer pendant plus longtemps qu'en temps réel, une fonction fort utile pour l'archivage : les images couleur haute résolution 700 x 480 à deux images par seconde utilisent 400 kbit/s par caméra. La souplesse d'attribution de largeur de bande du mappeur vidéo JungleMUX permet l'enregistrement d'images de meilleure résolution et d'un plus grand nombre d'images par seconde pour une caméra en particulier, en tout temps (jusqu'à une qualité de diffusion de 700 x 480, 30 images/s, signaux couleur NTSC, utilisant environ 6 Mbit/s [qualité MPEG-2]). Le système offre même des voies audio pour bruit ambiant pour les applications de surveillance publique.

La surveillance urbaine atteindra un tout nouveau plateau de contrôle, dès qu'un logiciel fiable de reconnaissance des visages deviendra la norme. Ce logiciel sera d'abord déployé dans les

Encadré 3 :

Technologie « neutre » sur la place Tienanmen

Après le massacre de la place Tienanmen en 1989, les autorités chinoises ont torturé et interrogé des milliers de personnes pour tenter d'identifier les organisateurs de la manifestation. Même si les étudiants et les travailleurs avaient résisté au régime de terreur de la police secrète, les infortunés manifestants n'avaient aucune chance de rester dans l'anonymat. La place Tienanmen est surveillée par un réseau de caméras fabriquées au Royaume-Uni, conçues pour surveiller et régulariser la circulation. Ces caméras ont enregistré toutes les activités des mois précédant l'arrivée des tanks sur la place.

Dans les jours qui suivirent, les images prises par ces caméras furent diffusées à répétition sur la chaîne de télévision nationale. Presque tous les transgresseurs furent ainsi identifiés. Siemens Plessey, fabricant et exportateur des caméras, et la Banque mondiale, qui a payé pour leur installation, prétendent qu'ils n'avaient aucune idée que leur équipement « technologiquement neutre » serait utilisé à ces fins. Toutefois, en 1995, la Banque mondiale a accordé les fonds pour établir le même système de contrôle de la circulation à Lhassa, la capitale de la Région autonome du Tibet, qui jusqu'ici ne s'est jamais plainte de problème d'embouteillage. En outre, la zone surveillée par le système de contrôle de la circulation est entièrement réservée à l'usage des piétons.[56]

emplacements comme les tourniquets, les douanes et les passages de sécurité pour assurer la reconnaissance standard du visage vu de face. C'est le début d'une révolution en surveillance algorithmique – l'application efficace de l'intelligence artificielle à l'analyse de données au moyen d'algorithmes complexes permettant la reconnaissance et le suivi automatiques. Une telle automatisation ne fait pas qu'élargir le filet de surveillance, elle en rétrécit les mailles.[58]

Au premier rang de cette révolution : AcSys Biometrics Corp., une entreprise en participation de AND Corporation, inventeur et développeur de la technologie d'intelligence artificielle Holographic/Quantum Neural Technology, HNeT, et de NEXUS, une société de gestion de Burlington en Ontario exploitant un réseau très diversifié de filiales autonomes et de partenariats.[59] AcSys Biometrics est un fournisseur d'un des systèmes de reconnaissance des visages les plus évolués sur le marché. Le Système de reconnaissance des visages d'AcSys (Face Recognition System (FRS)) fait maintenant partie de la gamme des produits de Nortel. Il est basé sur une technologie exclusive visant à établir rapidement et de manière fiable l'identité des personnes. Il s'agit d'une solution évolutive facile à intégrer aux systèmes et aux applications en place utilisant des protocoles réseau standard.

En rapport avec la stratégie Internet Personnel, Rick Collins, premier directeur, ProtoNet: Disruptive Solutions Implementation, à Nortel Networks, affirme que l'intégration des fonctions de reconnaissance des visages d'AcSys aux solutions de Nortel Networks rendra encore plus personnels les réseaux de communication. Les gens pourront être reconnus à l'emplacement. On ne devra plus, pour ce faire, utiliser des services mobiles. Il envisage un réseau qui sait qui vous êtes, éventuellement où vous êtes, et qui peut vous joindre que vous utilisiez un téléphone mobile ou un PC.[60]

Le système de reconnaissance de la parole et des visages d'AcSys Biometrics repose sur un module breveté d'intelligence artificielle appelé Holographic/Quantum Neural Technology (HNeT). Les réseaux neuronaux HNeT pourraient prendre en charge un grand nombre d'applications de Nortel dans les secteurs financier, manufacturier, médical, de la sécurité et

de la surveillance. Les technologies comme HNeT, permettant des vitesses d'apprentissage de 200 fois celle des réseaux neuronaux classiques, rendent bel et bien réelle la reconnaissance des visages sur CCTV et sont perçues par les pays dotés d'infrastructures CCTV comme une évolution naturelle de leurs réseaux. Comme le démontre l'exemple des systèmes de contrôle de la circulation installés sur la place Tienanmen et à Lhassa, l'amélioration des fonctions des systèmes de surveillance signifie une subtile érosion des droits humains. Les dynamiques de ce processus sont simples : le développement continuel de la technologie et l'utilisation de celle-ci à des fins autres que celles prévues.

Diagramme 1 :

Un nouveau modèle pour Internet : l'innovation à l'extrémité du réseau

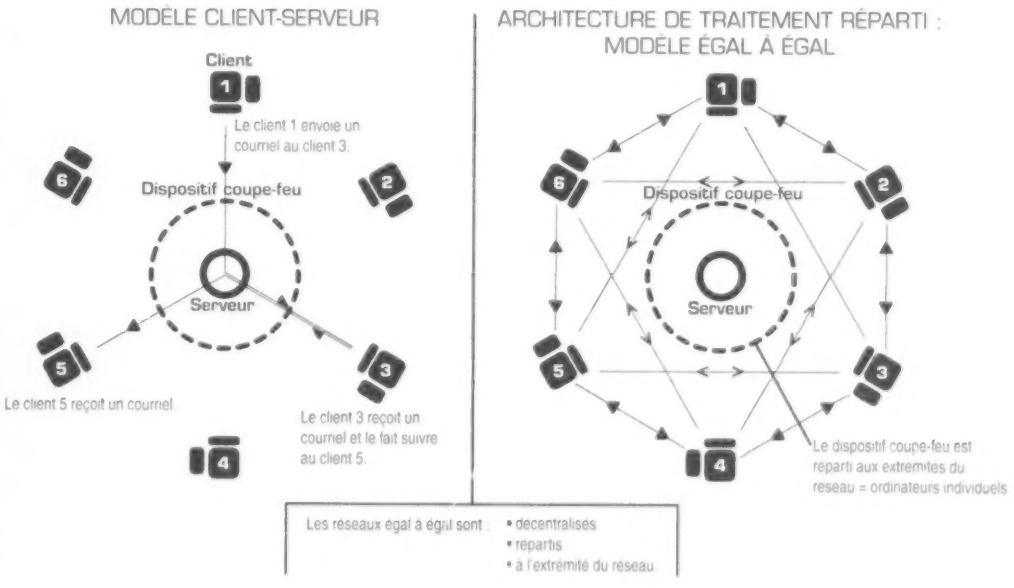
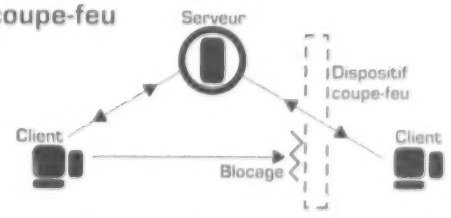


Diagramme 2 :

Interaction en présence d'un dispositif coupe-feu

Le logiciel d'égal à égal permet aux utilisateurs de communiquer directement entre eux par défaut. Quand un dispositif coupe-feu rend la communication directe impossible, la plupart des logiciels d'égal à égal dirigent automatiquement les messages vers un service de relais centralisé, pour l'acheminer sous tunnel vers l'accès 80.



Conclusion

« La souris est plus forte que le missile »

La seule chose qui distingue la stratégie Internet Personnel de Nortel, la recherche sur la reconnaissance de la parole ou la technologie CCTV des instruments de répression est la responsabilité démocratique. En Chine, les concepts de « sécurité de l'État » et de « secrets d'État », qui sont le fondement de la réglementation sur le contenu Internet et qui obligent les fournisseurs de services à surveiller les utilisateurs, ont toujours été utilisés pour restreindre la liberté d'expression, bloquer les organismes indépendants et supprimer de l'information. En Chine, le droit à la vie privée n'existe pas et aucun recours légal n'existe non plus pour tenir le gouvernement responsable de son utilisation de l'information obtenue par son appareil de sécurité au moyen de la surveillance, de l'écoute en ligne ou de la surveillance en ligne de communications électroniques.

En Chine, comme dans tous les pays du monde, les activistes qui se portent à la défense des droits humains livrent un nouveau combat : s'assurer que l'innovation technologique est au service de la liberté et de la démocratie et ne devient pas une forme subtile et évoluée de répression. Bon nombre des entreprises qui exposent leur marchandise au salon Security China 2000 prétendent partager cet objectif en soutenant qu'elles agissent pour améliorer la qualité de vie et de travail des gens (Philips) et pour que les gens puissent rester en contact, partout et en tout temps, avec les ressources dont ils ont besoin (Sun Microsystems).

Dans la pratique, toutefois, d'autres mesures ont besoin d'être mises en place pour que ces belles phrases soient plus qu'un simple exercice de relations publiques. Tandis que les prédicateurs de la mondialisation parlent de « règles du jeu équitables » et de « systèmes basés sur des règles », des millions de gens en Chine vivent dans un système de contrôle politique qui a un impact sur chaque aspect de leur vie. On ne peut parler de règles du jeu équitables sans liberté, ni de systèmes basés sur des règles lorsque ces règles ne gouvernent que la dimension commerciale de l'interaction humaine et que l'État viole constamment les droits humains fondamentaux.

Les gouvernements démocratiques, dont celui du Canada, doivent donner la priorité à la promotion des droits humains dans tous les aspects de leurs relations internationales, incluant les échanges commerciaux et les investissements. En 1995, dans son énoncé de politique étrangère *Le Canada dans le monde*, le gouvernement du Canada proclamait son engagement : «... nous utiliserons efficacement toute l'influence que nous confèrent nos relations économiques et commerciales et notre aide au développement pour promouvoir le respect des droits de la personne. »

Devant un forum d'organisations non gouvernementales tenu à Montréal en 1998, le ministre canadien des Affaires étrangères et du Commerce international, Lloyd Axworthy, avait tenu les propos suivants :

« Nous sommes ici pour discuter d'une technologie qui révolutionne le monde – qui modifie les rapports de force, remet en question les circuits de communication conventionnels, répand et dissémine au maximum l'influence – et démocratise ainsi les voies de transmission en se débarrassant de ceux qui veulent les contrôler... parce que le potentiel de cette technologie de forcer les barrières, de surmonter les obstacles d'ordre politique – d'éduquer, d'informer et d'être un agent de changement politique – est proprement ahurissant... la souris est plus forte que le missile. »[61]

Malheureusement, en Chine, la technologie ne sert pas une cause aussi noble. Les multinationales au premier rang de la révolution de l'information ne peuvent prétendre que leur seule présence en Chine garantira un meilleur respect des droits humains; les gouvernements ne peuvent s'obstiner à croire que les marchés ouverts mèneront automatiquement à la démocratie. Dans les pays à régime autoritaire et oppressif où la lutte contre le crime est volontairement confondue avec la répression de la dissidence, des règles différentes doivent être appliquées pour orienter le développement politique et social. Ignorer ce défi, c'est compromettre la liberté en Chine, certes, mais c'est aussi, dans nos sociétés en voie de mondialisation, mettre en péril la liberté de tous.

Annexe

Comment utiliser le CD-ROM qui accompagne le présent document

Installation :

Suivez les instructions ci-dessous pour installer le CD-ROM pour Windows 95/98/ME/2000 et Mac OS.

1. Fermez toutes les applications et ouvrez le lecteur de CD-ROM.
2. Déposez le CD-ROM dans le lecteur, face graphique vers le haut.
3. Une fois le lecteur fermé, une fonction d'exécution automatique lance le programme d'installation.

Si votre ordinateur n'est pas doté d'une telle fonction ou que cette fonction est désactivée, vous pouvez lancer le programme d'installation, appelé chinags.exe, comme suit :

Windows : Double-cliquez sur l'icône Poste de travail de votre bureau. Double-cliquez ensuite sur l'icône correspondant à votre lecteur de CD-ROM puis sur l'icône chinags.exe.

Mac : Cliquez sur l'icône CD-ROM du bureau puis sur l'icône chinags.exe.

Textes de la pochette

> ***Les moyens de distribution de ce rapport – surtout sa version chinoise – sont aussi importants que le contenu du rapport lui-même.***

> **En raison de la législation régissant Internet en Chine – surtout en ce qui concerne notre obligation de fournir l'accès aux lecteurs chinois – et au cours de la recherche et de la distribution de ce rapport, un certain nombre d'outils et de concepts libres ont été utilisés. Ils sont expliqués brièvement ci-dessous.**

> **Si vous voulez accéder à la version en ligne de ce rapport (à go.openflows.org) à partir de la Chine, veuillez utiliser le logiciel anticensure-antisurveillance fourni sur le CD-ROM.**

> **La version en ligne du rapport ainsi que celle fournie sur le CD-ROM comportent des renseignements supplémentaires sur le processus de recherche, y compris un aperçu des règlements et de la législation de la Chine régissant les communications électroniques.**

Appel à l'action

Cette année, à la conférence Linux World, Lawrence Lessig, professeur de droit à l'Université de Stanford, a lancé le défi de s'engager et de combattre le pouvoir des « anciens ».[62]

Lessig, célèbre pour sa contribution au droit Internet et auteur du livre *Code and Other Laws of Cyberspace*, a décrit comment une législation désuète, le monde financier, le gouvernement et les grandes entreprises ont détourné à leur profit la « plate-forme libre » que devait être Internet, idéologiquement conçue pour favoriser la libre expression, mais devenue un outil de répression de l'innovation.

M. Lessig a demandé à son auditoire : « Que voulez-vous faire à ce sujet ? Je ne pourrai pas arrêter ce changement. Plus je parle et moins on (le gouvernement et les entreprises) veut m'écouter, moins on veut entendre cette histoire. Mes efforts sont inutiles dans cette lutte. Ceux qui peuvent faire une différence, c'est vous, les gens qui ont construit cette architecture de liberté. »

Hacktivismo !

« Hacktivismo et le CULT OF THE DEAD COW publient la présente déclaration pour exprimer leur indignation et affirmer leur intention d'agir. La déclaration Hacktivismo est notre Magna Carta pour le droit à l'information. La population a droit à un accès raisonnable à toute information publiée légalement. Si nos dirigeants ne sont pas prêts à défendre Internet, nous le sommes. »

« A Special Message of Hope », 4 juillet 2001[63]

Patrick Ball

« L'Hacktivismo place la technologie au service des droits humains », selon Patrick Ball, directeur adjoint du programme Human Rights de l'American Association for the Advancement of Science, qui a participé entre autres à des projets d'enquête des Nations Unies sur les crimes de guerre et les génocides ainsi qu'à des projets sur les droits humains au Guatemala, en Haïti et en Afrique du Sud.

PGP

De nombreux groupes de défense des droits humains utilisent des logiciels de cryptographie ou de chiffrement comme PGP (Pretty Good Privacy) pour protéger leurs messages, ce qui est souvent une question de vie ou de mort. PGP empêche l'information de tomber entre les mains de personnes autres que les destinataires et vérifie si les messages sont authentiques au moyen de signatures numériques. Son impact sur le respect des droits humains est énorme. [Voir CD-ROM.]

Rubberhose

(prononcé Marutukku)

Rubberhose a d'abord été conçu par le programmeur en cryptographie Julian Assange comme outil pour les militants des droits de la personne et les journalistes qui devaient protéger des données confidentielles comme des listes d'activistes ou des détails concernant des violations de droits.

Les programmeurs de Rubberhose ont rencontré des groupes de militants des droits humains et entendu des récits de ces violations. Les militants doivent souvent transporter, dans des situations extrêmement dangereuses, des portables contenant des données essentielles. Ils sont parfois arrêtés par des patrouilles militaires qui n'hésiteraient pas à torturer un suspect pour obtenir le mot de passe leur permettant d'accéder aux données.

Freenet

Freenet est un énorme réseau P2P qui regroupe la puissance des ordinateurs membres dans le monde entier pour créer un dépôt d'archives ouvert à tous ceux qui désirent publier ou consulter des renseignements de tout type. La version 1.0 du présent rapport est publiée en trois langues sur Freenet. Elle est accessible à la Chine et au reste du monde. [Voir CD-ROM.]

SafeWeb

Internet en Chine, le catalyseur d'un changement social ?

SafeWeb est un service mandataire anonyme à chiffrement SSL actuellement utilisé environ 100 millions de fois par mois par des centaines de milliers de personnes dans le monde. Il est le site Web le plus populaire au monde.

Triangle Boy est un programme libre qui permet à des bénévoles de transformer leur PC en passerelle dans le réseau SafeWeb afin d'empêcher les gouvernements répressifs de censurer Internet. Triangle Boy a recours à des techniques de contrefaçon d'adresses IP et de transmission par paquets pour réduire la consommation de largeur de bande sur les ordinateurs des bénévoles. [Diagramme 2 : Interaction en présence d'un dispositif coupe-feu.]

Glossaire

Acheminement (tables d'acheminement)
Processus permettant de diriger les paquets entre les points d'origine et de destination dans un système interconnecté. L'acheminement est généralement effectué par un dispositif spécialisé appelé *routeur*. La fonction d'acheminement est une fonction importante du réseau Internet parce qu'elle permet de relayer les données d'un ordinateur à un autre, jusqu'à ce qu'elles parviennent à destination. Les ordinateurs intermédiaires accomplissent cette tâche en transmettant les données reçues au prochain ordinateur. Pour déterminer le meilleur parcours, les ordinateurs consultent des tables d'acheminement.

Adresse IP
Numéro unique composé de quatre groupes de chiffres séparés par des points. Exemple : 163.113.245.2.
Tous les ordinateurs reliés à Internet sont identifiés par une adresse IP unique. Un ordinateur qui n'est pas identifié par une adresse IP n'est pas vraiment relié à Internet. La plupart des ordinateurs sont également identifiés par un nom de domaine, plus facile à mémoriser.

ADSL (ligne numérique à paire asymétrique)
Technologie qui permet de transmettre des données sur les lignes téléphoniques classiques. Beaucoup plus rapide que le service téléphonique ordinaire, la technologie ADSL utilise la même paire de fils de cuivre que le service téléphonique ordinaire. Le circuit ADSL doit être configuré pour relier deux emplacements particuliers, comme une ligne spécialisée. L'ADSL peut atteindre des vitesses de téléchargement de 1,544 Mbit/s, en direction de l'usager, et de 128 kbit/s, en direction du réseau.

ATM (mode transfert asynchrone)/Relais de trames

Une technologie réseau souple de multiplexage et de commutation offrant une largeur de bande variable aux réseaux locaux (LAN) et longue distance (WAN). Contrairement aux configurations synchrones ordinaires, ATM permet l'attribution flexible de la largeur de bande disponible pour la transmission de données, de la voix et d'images vidéo. ATM utilise une architecture évolutive, ce qui facilite sa mise à niveau. Ce mode permet à un nombre virtuellement illimité d'usagers d'utiliser des liaisons haute vitesse spécialisées raccordées à des serveurs réseau à haut rendement. Des études d'ingénierie indiquent que ATM peut, en théorie, prendre en charge des débits de 622 Mbit/s sur fibre optique et de 155 Mbit/s sur fil de cuivre classique.

« Boîte noire »
Dispositif que les fournisseurs de services Internet (FSI) installent sur leurs serveurs pour envoyer à un organisme de sécurité gouvernemental une copie des données transmises par leur système.

Carte intelligente
Petit dispositif électronique, ayant à peu près la taille d'une carte de crédit, qui contient une mémoire électronique et parfois un circuit intégré. Les cartes contenant un circuit intégré sont également appelées *cartes de circuits intégrés (CCI)*.
Les cartes intelligentes sont utilisées dans différentes applications, telles que :

> stockage des informations médicales d'un patient ;
> argent électronique ;
> génération d'identificateurs de réseau.

CDMA (accès multiple à répartition par codes)
Technologie de transmission utilisée avec les services numériques sans fil pour transmettre la voix ou les données. Cette technologie, basée sur un procédé d'étalement du spectre, est de plus en plus utilisée partout dans le monde. La société Datang a mis au point une version chinoise de cette technologie, appelée TD-SCDMA.

Compression (algorithme)
La compression est un procédé qui permet de diminuer la taille d'un fichier ou d'un train de données afin d'accroître la vitesse de transmission ou de réduire l'espace de stockage.
Un algorithme est une formule ou une séquence d'instructions utilisée pour résoudre un problème particulier. Il est constitué d'un ensemble de règles non ambiguës qui aboutissent à un résultat clairement défini.
Une recette de gâteau, par exemple, est un algorithme. La conception d'algorithmes efficaces, c'est-à-dire simples et comportant le moins d'étapes possible, est un des principaux défis de la programmation.

Contrefaçon d'adresses IP
Technique qui permet d'accéder à un ordinateur en envoyant des données identifiées par une fausse adresse IP qui semble être celle d'un système sûr. Pour ce faire, un pirate informatique utilise une des nombreuses techniques à sa disposition pour trouver l'adresse IP d'un système sûr, puis tromper l'ordinateur en remplaçant l'adresse d'origine par l'adresse « sûre » dans les en-têtes des paquets. Les nouvelles configurations de coupe-feu et les nouveaux routeurs offrent maintenant une protection contre ce type de contrefaçon.

Convergence
Fusion d'au moins deux disciplines ou technologies distinctes. Par exemple, le télécopieur a vu le jour grâce à trois technologies convergentes, les télécommunications, le balayage optique et l'impression. D'une façon plus générale, la convergence désigne la rencontre de la télévision, de l'ordinateur personnel et d'Internet pour constituer ce qu'il est convenu d'appeler « les nouveaux médias ».

Courrier poubelle (pourriel)
Courriel non sollicité transmis à un grand nombre de destinations.

Diffusion multimédia en temps réel
Technique de transfert de données qui permet de transmettre des données en un flux continu à un débit constant. Avec la croissance d'Internet, les technologies de diffusion en temps réel jouent un rôle de plus en plus important, car la plupart des utilisateurs ne disposent pas d'une connexion permettant de transmettre rapidement des fichiers multimédias de grande taille. Grâce à la diffusion en temps réel, le navigateur ou le module complémentaire client peut commencer à afficher les données avant que le fichier ne soit complètement transmis.

Dispositif coupe-feu
Système permettant d'empêcher des personnes non autorisées d'accéder à un réseau ou de transmettre des données à l'extérieur d'un réseau. Les dispositifs coupe-feu peuvent être du type matériel ou logiciel ou une combinaison des deux, et ils sont souvent utilisés pour bloquer l'accès à des réseaux privés reliés à Internet, notamment les intranets. Toutes les communications qui pénètrent l'intranet ou qui en sortent sont analysées par le dispositif coupe-feu, qui bloque celles qui ne respectent pas les règles définies. Il existe plusieurs types de dispositifs coupe-feu :

> **Filtrage de paquets :** Le dispositif coupe-feu analyse tous les paquets qui pénètrent dans le réseau ou qui en sortent et les accepte ou les rejette en se basant sur des règles définies par l'utilisateur. Le filtrage des paquets est un système efficace et transparent pour l'utilisateur, bien qu'il soit difficile à configurer. En outre, il est très vulnérable aux procédés de contrefaçon d'adresses IP.
> **Passerelle d'application :** Applique des mécanismes de sécurité à certaines applications, comme les serveurs FTP et Telnet. Cette méthode est très efficace, mais elle réduit la performance du système.
> **Serveur mandataire :** Intercepte toutes les communications qui pénètrent dans le réseau ou qui en sortent. Ce type de serveur cache efficacement les adresses réseau réelles.

En pratique, il n'est pas rare que les dispositifs coupe-feu utilisent deux ou plus de deux méthodes de protection. Le dispositif coupe-feu est la première ligne de défense pour la protection des informations confidentielles. Au besoin, il est possible de chiffrer les données pour augmenter le niveau de sécurité.

Égal à égal
Type de réseau dans lequel chaque ordinateur possède les mêmes capacités et responsabilités. Ce type de réseau est très différent d'une architecture client-serveur dans laquelle la fonction de certains ordinateurs est strictement de desservir d'autres ordinateurs. Les réseaux d'égal à égal sont en général de configuration plus simple mais ils n'offrent pas la même performance système pour les grands volumes de trafic sur large bande.

Fibre optique
Dispositif utilisé pour transmettre des communications au moyen de fibres souples pouvant transmettre la lumière.

Filtrage des paquets
Procédé permettant de contrôler l'accès à un réseau qui consiste à analyser les paquets entrants et sortants et à laisser passer ou à bloquer des paquets en se basant sur les adresses IP (protocole Internet) du point d'origine et de la destination. Le filtrage des paquets est l'une des techniques utilisées pour créer des dispositifs coupe-feu.

Gbit/s

Gigabit par seconde. Unité de mesure de la vitesse de transmission des données représentant 1 000 000 000 de bits par seconde. Cette unité est utilisée, par exemple, pour les réseaux à grande vitesse, tels qu'Ethernet gigabit.

Immeubles intelligents

Les immeubles intelligents sont munis de dispositifs électroniques qui prennent en charge :

> la consommation d'énergie ;
> les dispositifs de sécurité ;
> les systèmes de télécommunication ;
> l'automatisation des lieux de travail.

L'objectif ultime est de concevoir un immeuble intelligent qui réunit les quatre grandes fonctions de gestion électronique de l'immeuble en un seul système informatisé intégré, basé sur le logiciel et le matériel d'un fournisseur unique.

IP

Acronyme qui signifie *protocole Internet*. Ce protocole spécifie le format des paquets, parfois appelés datagrammes, ainsi que le mode d'adressage. La plupart des réseaux combinent le protocole IP avec un protocole de plus haut niveau, appelé TCP (*Transmission Control Protocol – Protocole de contrôle de transmission*), qui établit une connexion virtuelle entre un point d'origine et une destination.

Le protocole IP fonctionne un peu comme le système postal. Il permet d'attribuer une adresse à un message, puis de le mettre à la poste, sans qu'il soit nécessaire d'établir un lien direct entre l'expéditeur et le destinataire. Par contre, le protocole TCP/IP établit une connexion entre deux points, qui peuvent alors échanger des messages. La version actuelle du protocole Internet est *IPv4*. Une nouvelle version, appelée *IPv6*, est en cours de développement.

Large bande

Se dit d'un service utilisant une plage de fréquences étendue et pouvant fournir simultanément plusieurs voies de communications. La fibre optique, par exemple, offre beaucoup de largeur de bande.

Largeur de bande

Largeur de la plage de fréquences d'une voie de transmission. Ce terme est souvent utilisé pour désigner la quantité de données pouvant être transmise par un circuit. Plus la largeur de bande est grande, plus la quantité de données pouvant être transmise pendant une durée déterminée est grande.

Quel volume de données peut-on transmettre par une connexion ? Ce volume est généralement exprimé en bits par seconde. Par exemple, une page de texte nécessite environ 16 000 bits. Un modem rapide peut transmettre environ 15 000 bits par seconde. La transmission d'images vidéo animées exige environ 10 000 000 de bits par seconde, selon le type de compression.

Mbit/s

Mégabit par seconde (million de bits par seconde). Unité utilisée pour mesurer la vitesse de transmission des données. La vitesse des réseaux modernes, par exemple, est généralement supérieure à un mégabit par seconde.

Mux (multiplexeur)

Dispositif permettant de combiner des signaux multiples (analogiques ou numériques) et de les acheminer sur un circuit de transmission. Par exemple, un type de multiplexage très répandu combine plusieurs signaux à basse vitesse et les achemine sur une seule ligne de transmission à grande vitesse.

Passerelle

Une passerelle, également appelée *logiciel mandataire*, est un programme d'application tournant sur un dispositif coupe-feu installé entre deux réseaux. Lorsqu'un client veut établir une connexion avec une destination, il établit d'abord la connexion avec la passerelle, puis négocie avec celle-ci pour communiquer avec la destination. La passerelle établit ensuite la connexion avec la destination derrière le coupe-feu et agit au nom du client, cachant et protégeant les ordinateurs du réseau derrière le coupe-feu. Cette méthode établit donc deux connexions, l'une entre le client et la passerelle, l'autre entre la passerelle et la destination réseau. Lorsque la connexion est établie, la passerelle prend en charge l'acheminement des paquets. Puisque toutes les communications passent par la passerelle, les ordinateurs qui se trouvent derrière le coupe-feu sont protégés. Ce procédé est considéré comme très sûr, mais il exige beaucoup plus de ressources de processeur et de mémoire que les autres types de coupe-feu.

Qualité télécommunicateur

Terme qui désigne des équipements réseau offrant le niveau de fiabilité élevé requis par les fournisseurs de services Internet (FSI). L'équipement de qualité télécommunicateur affiche des pourcentages de fiabilité de 99,999 % et plus.

Réseau intranet, réseau national ou réseau à l'échelle de la Chine

Réseau privé utilisant les mêmes logiciels que le réseau Internet public mais réservé à l'usage d'une entreprise ou d'un organisme. En raison de la popularité croissante d'Internet, plusieurs outils internetisés sont maintenant utilisés dans les réseaux privés. En outre, bon nombre d'entreprises disposent maintenant de serveurs Web réservés à l'usage de leur personnel.

Réseau

Système composé de deux ordinateurs ou plus reliés les uns aux autres. Il existe plusieurs types de réseau, notamment :

> **Réseau local (RL ou LAN) :** Les ordinateurs sont relativement près les uns des autres, par exemple, dans le même immeuble.

> **Réseau longue distance (RLD ou WAN) :** Les ordinateurs sont plus éloignés les uns des autres et sont reliés par des lignes téléphoniques ou des câbles de fibres optiques.

En plus des types de réseau, certaines autres caractéristiques sont utilisées pour classer les réseaux :

> **Topologie :** La configuration géométrique des connexions qui relient les ordinateurs entre eux (bus, étoile, anneau, etc.).

> **Protocole :** Le protocole définit un certain nombre de règles et de signaux qui permettent aux ordinateurs de communiquer entre eux sur un réseau. Un des protocoles les plus courants porte le nom d'*Ethernet*. Le protocole *Anneau à jetons d'IBM* est un autre protocole souvent utilisé pour relier les PC.

> **Architecture :** Les réseaux peuvent être classés selon leur architecture, qui peut être du type *égal à égal* ou *client-serveur*.

Les ordinateurs d'un réseau sont parfois appelés *nœuds*. Les ordinateurs et les dispositifs qui fournissent des ressources à un réseau sont appelés *serveurs*.

Réseau principal

Ligne ou série de connexions constituant une voie de transmission principale dans un réseau. Toutefois, cette notion est relative, car la voie principale d'un petit réseau sera probablement d'une taille de beaucoup inférieure à celle de certaines voies secondaires dans un grand réseau.

RPV (réseau privé virtuel)

Réseau privé qui utilise le réseau téléphonique public pour relier des ordinateurs en réseau. Par exemple, bon nombre de systèmes permettent de créer un réseau en utilisant Internet pour transporter les données. Ces systèmes utilisent le chiffrement et d'autres mesures de sécurité pour empêcher des personnes non autorisées d'accéder au réseau ou d'intercepter les données.

Serveur mandataire

Serveur situé entre une application client, comme un navigateur Web, et un serveur réel. Le serveur mandataire intercepte toutes les demandes dirigées vers le serveur réel et les lui transmet, si possible, ou y répond lui-même.

TCP/IP

Acronyme signifiant *protocole de contrôle de transmission/protocole Internet*, un ensemble de protocoles de communication utilisés pour relier des ordinateurs à Internet. Le protocole TCP/IP comprend plusieurs protocoles, dont les principaux sont TCP et IP. Le protocole TCP/IP est intégré au système d'exploitation UNIX et est utilisé sur Internet, ce qui en fait la norme de facto pour la transmission des données sur les réseaux. Même les systèmes d'exploitation réseau qui utilisent leurs propres protocoles sont compatibles avec le protocole TCP/IP.

Télécommunicateur

Entreprise de télécommunications qui revend des services de communications à d'autres entreprises.

Traitement des paquets

Un paquet est un groupe de données transmis au moyen d'un réseau de commutation de paquets. En plus des données, un paquet contient l'adresse de sa destination. Dans les réseaux IP, les paquets sont souvent appelés *datagrammes*.

Notes en fin d'ouvrage

[1] HONG KONG IS SWALLOWED UP, de Jeff Jacoby, *The Boston Globe*: http://www.bigeye.com/jj070197.htm
CHINESE CHECKERS, OxBlood Ruffin, CDC
http://www.cultdeadcow.com/cDc_files/cDc-0361.html
The Money Trap, une recension de Robert Kagan
Réimpression avec la permission de *The New Republic*
Première publication le 7 avril 1997
http://www.ceip.org/people/kagrep1.htm

[2] Voir la note 59.

[3] http://www.hrw.org/backgrounder/asia/china-bck-0701.htm. Freedom of Expression and the Internet in China, A Human Rights Watch Backgrounder

[4] Dr Hsu citant un sondage de l'Académie chinoise des sciences sociales (CASS) – Dr Guo Liang, *China Academy of Social Sciences*, mai 2001

[5] (CHINANET, CHINGBN, CERNET, CSTNET et UNINET)
[Voir diagramme 1 : Un nouveau modèle pour Internet : l'innovation à l'extrémité du réseau.]

[6] Traduction de « *churukou xindao* »

[7] Voir, par exemple, http://www.wirednews.com/wired/5.06/china_pr.html
5.06 – Juin 1997, *The Great Firewall of China*, Geremie R. Barme et Sang Ye

[8] Big Brother Incorporated, Privacy International: http://www.privacy.org/pi/reports/

[9] http://www.cpsr.org/alert/cpsr.alert.2.05.html. Volume 2.05, 12 novembre 1993, publié par Computer Professionals for Social Responsibility
Washington Office
(Alert@washofc.cpsr.org)
Documents « Operation Root Canal » publiés : Questions Raised about FBI's Digital Telephony Initiative
« In response to a CPSR Freedom of Information Act lawsuit, the FBI this week released 185 pages of documents concerning the Bureau's Digital Telephony Initiative, code-named Operation "Root Canal." The newly disclosed material raises serious doubts as to the accuracy of the FBI's claim that advances in telecommunications technology have hampered law enforcement efforts to execute court-authorized wiretaps. »

[10] Source :
http://www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html.
Nortel a depuis retiré cette URL de son site Web. Toutefois, une copie de la page d'origine demeure dans la cache Web de Google. On peut la consulter à :
http://www.google.com/search?q=cache:Ijjs4pWPJ8Y:www.nortelnetworks.com/products/01/dms-10/dms10news/august99/article6.html.
« Nortel has been actively involved in ad hoc committees established prior to the law being enacted. We have been active participants during the standards process with technical representatives at key meetings. »

[11] Version finale du projet de loi adopté par les deux assemblées législatives :
http://thomas.loc.gov/cgi-bin/query/z?c103:H.R.4922.ENR: H.R.4922
To amend title 18, US Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other...

[12] *Ibid*, texte tiré de la CALEA

[13] http://www.askcalea.net/about/doj990914.htm
Department of Justice and FBI Reach First Agreement Under Communications Assistance for Law Enforcement Act

[14] http://www.askcalea.com/about/pl103414.htm
« (1) IN GENERAL- A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify. »

[15] http://www.bc.edu/bc_org/avp/law/st_org/iptf/headlines/content/1997013101.html
1997 B.C. Intell. Prop. & Tech. F. 013101
Government Tempers Electronic Surveillance Proposal; Critics Laud Changes But Are Not Satisfied
par Adam White Scoville, rédacteur
Voir aussi : http://www.cdt.org/publications/pp_3.01.html
CDT POLICY POST Volume 3, Numéro 1, 17 janvier 1997

[16] Voir échéancier ENFOPOL : http://www.heise.de/tp/english/special/enfo/6382/1.html
Voir aussi : UE *Document 496Y1104(01)*
http://europa.eu.int/eur-lex/fr/lif/dat/1996/fr_496Y1104_01.html
« considérant que, selon une décision prise par les ministres "TREVI" en décembre 1991, une étude devrait être effectuée en ce qui concerne les conséquences de l'évolution juridique et technique et de l'évolution du marché dans le domaine des télécommunications à l'égard des différentes possibilités d'interception et en ce qui concerne les mesures à prendre afin de faire face aux problèmes qui ont surgi... »

[17] Pour obtenir le texte intégral de tous les documents ENFOPOL cités dans le présent document, rendez-vous à http://www.statewatch.org/eufbi/index.html.
A sa première réunion à Bruxelles les 29 et 30 novembre 1993, le nouveau Conseil des ministres de la Justice et de l'Intérieur a adopté la résolution suivante sur l'interception des communications. Elle parle d'elle-même et est reproduite en entier ici en anglais:
« RÉSOLUTION DU CONSEIL SUR L'INTERCEPTION DES TÉLÉCOMMUNICATIONS
Le Conseil
1. demande au groupe d'experts de comparer les besoins des États membres de l'Union à ceux du FBI;
2. convient que, pour éviter un débat axé uniquement sur les besoins du FBI, ceux des États membres de l'Union seront communiqués aux pays tiers qui ont participé à la réunion du FBI à Quantico (notamment la Suisse, la Norvège, la Finlande [pays ayant fait une demande d'accession à la Communauté européenne], les États-Unis et le Canada) et qui sont mentionnés dans le protocole approuvé par les ministres lors de leur réunion tenue à Copenhague;
3. approuve pour des raisons pratiques que la décision sur la coopération des pays tiers prise à la réunion des ministres à Copenhague s'applique également à Hong Kong, à l'Australie et à la Nouvelle-Zélande (ayant participé à la réunion du FBI);
4. par les présentes décide que des discussions non officielles avec les pays précités peuvent être envisagées : à cette fin, la présidence et le groupe d'experts peuvent, par exemple, organiser une rencontre avec ces pays tiers pour échanger de l'information. »

[18] Voir www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf:
SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA
DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE
OF ECONOMIC INFORMATION
Vol. 5/5: The perception of economic risks arising from the potential vulnerability of
electronic commercial media to interception

[19] http://www.oneworld.org/index_oc/issue198/codewar.html: The code war
David Banisar et Simon Davies. David Banisar est un avocat du Electronic Privacy Information Center (EPIC) à Washington, DC, directeur adjoint de Privacy International (PI) et coauteur d'un nouveau livre sur la politique de chiffrement: *The Electronic Privacy Papers: The Battle for Privacy in the Age of Surveillance*. Simon Davies est directeur général de PI, auteur de *Big Brother* et visiteur stagiaire de la London School of Economics.

[20] www.europarl.eu.int/stoa/publi/pdf/981401-5en_en.pdf

[21] http://www.statewatch.org/eufbi/index.html

[22] Draft COUNCIL RESOLUTION on the lawful interception of telecommunications in relation to new technologies ENFOPOL 19, 15 mars 1999 : http://www.fipr.org/polarch/enfopol19.html

[23] What do YOU want the Internet to be? http://www.nortelnetworks.com/corporate/internet/what_do_you_want/index.html

[24] China looks for new technology to police Net
par Martin Fackler, Associated Press, 9 novembre 2000

[25] http://www.adsaleexh.com/sec/press2.html
Communiqué, 29 août 2000
Over 300 International Exhibitors Gather in Security China 2000
Taping the Lucrative China Market

[26] *Ibid*

[27] http://www.adsaleexh.com/sec/press1.htmmime text/html
Communiqué, 10 mars 2000
The No. 1 International Security Exhibition back to Beijing again

[29] *Ibid*, Adsale

[29] *Ibid*, Adsale

[30] Research Overview, Speech Signal Processing and Intelligence Technology Group Department of Electronic Engineering, Tsinghua University
http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm
Tsinghua a depuis retiré cette URL de son site Web. Toutefois, une copie de la page d'origine demeure dans la cache Web de Google. On peut la consulter à :
http://www.google.com/search?q=cache:4Ew-AlksjbU:www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm+863+tsinghua+engineering+speech+continuous&hl=en

[31] *Ibid*

[32] http://www.most.gov.cn/English/Programs/863/menu.htm

[33] http://138.110.28.9/acad/intrel/chinmc.htm
EVAN A. FEIGENBAUM, China's Military-Civilian Complex, *New York Times*, 22 mai 1998

[34] *Ibid*, 27

[35] *Ibid*

[36] BNR exploite des laboratoires de recherche dans plusieurs pays, notamment deux au Canada (Ottawa et Montréal), trois aux États-Unis (Raleigh, Richardson et Atlanta), quatre au Royaume-Uni (Harlow, New Southgate, Maidenhead et Monkstown), un au Japon (Tokyo), un en Australie (Sydney) et un en Chine (Beijing).

[37] Nortel Networks signe des contrats évalués à plus de 120 millions de dollars US pendant la visite du premier ministre Jean Chrétien en Chine.
http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[38] http://www.ee.tsinghua.edu.cn/teachers/wangzuoying/research.htm

[39] Objectifs précis de conformité - J-STD-025 établit les normes pour la conformité de base à la CALEA :
voir Plate-forme série DMS-500 de Nortel, Document no : 51047-16-12-00.pdf.

[40] http://www.nortelnetworks.com/corporate/news/newsreleases/1998c/11_20_9898638_Chretien.html

[41] Plus de 100 millions $US dans le cas de Nortel selon le Département de la justice américain : voir www.doj.gov.

[42] http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

[43] Selon un rapport du 12 juin dans le quotidien *China Daily*.

[44] http://www.smartcards-china.com/en/page_ehydt1.htm[45]
http://www.state.gov/www/global/human_rights/1999_hrp_report/china.html
Site FTP pour information du *Department of State*, avant le 20 janvier 2001.
1999 Country Reports on Human Rights Practices
Publié par le Bureau of Democracy, Human Rights, and Labor
U.S. Department of State, 25 février 2000

[46] Signalé à Mingbao, information fournie par Judy Chen, HRIC

[47] http://www.telecomn.com/english/china_comm/CN_200010.htm *DATANG TELECOM CONTRACTS "INTELLIGENT BUILDING WEAK CURRENT ENGINEERING" FOR JILIN PROVINCIAL PUBLIC SECURITY DEPARTMENT*

[48] http://www.gzjd.gov.cn/gzjd/

[49] *Ibid*, AP

[50] China Online, http://www.chinaonline.com/topstories/001114/1/c00111456.asp

[51] http://www.nortelnetworks.com/corporate/events/2001b/myviewtour/plenary_fr.html

[52] « The idea that ISPs are watching where [customers] go is unacceptable... it's like the Post Office looking into your mail in order to decide what kind of junk to send you. » (Junkbusters.org) Plusieurs projets de loi sur la vie privée sont actuellement en cours d'introduction ou de réintroduction au Congrès des États-Unis et autres corps législatifs des États-Unis. Un des projets de loi à l'étude au Congrès, la Spyware Control and Privacy Protection Act, vise à protéger les utilisateurs en ligne contre la technologie Internet Personnel de Nortel. Évidemment, en Chine, le polluriel et le télémarketing sont les derniers des soucis.

[53] En plus d'OPTera Metro, la solution de Nortel pour Shanghai Telecom comprend le Shasta 5000 Broadband Service Node (BSN) et les autocommutateurs multiservices Passport 15000 et Passport 7480 de Nortel Networks.

[54] http://www.nortelnetworks.com/help/legal/index_fr.html#privacy

[55] *Ibid*

[56] AN APPRAISAL OF THE TECHNOLOGIES OF POLITICAL CONTROL, An Omega Foundation Summary & Options Report For The European Parliament, septembre 1998

[57] *Ibid* 22 (AP)

[58] (Voir Norris, C., et. al, 1998.)

[59] Nexus (www.nxsgrp.com et www.nxs.ca), anciennement Heritage Concepts International (HCI). NEXUS Group International Inc. AND Corporation (www.andcorporation.com). AcSys Biometrics Corp. (www.acsysbiometricscorp.com).

[60] http://www.andcorporation.com/press/press_3_12_01.html. AcSys Biometrics Accompanies Nortel Networks to CeBIT 2001

[61] Bob Paquin, article sur le site Web du journal *The Ottawa Citizen*, lundi 26 octobre 1998. E-Guerillas in the mist.

[62] Linux World Conference: http://www.linuxworld.com/

[63] http://www.cultdeadcow.com/cDc_files/declaration.html

« Si vous vous tenez toujours droit,
alors votre ombre ne sera jamais courbée. »
> Liu Qing, ancien prisonnier politique

Autres publications de Droits et Démocratie :
(Consultez notre site www.ichrdd.ca pour une liste complète de nos publications.)
Un cadre de référence des droits humains pour le commerce dans les Amériques, par Diana Bronson et Lucie Lamarche, 2001.
Le dialogue bilatéral avec la Chine affaiblit le système international de protection des droits humains, 2001.
Protection des droits humains et mondialisation de l'économie. Un défi pour l'OMC, par Robert Howse et Makau Mutua, 2000.
Les intérêts miniers canadiens et les droits de la personne en Afrique dans le cadre de la mondialisation, par Bonnie Campbell, 1999.
Les femmes et la consolidation de la paix, par Dyan Mazurana et Susan McKay, 1999.
Donner une conscience au commerce : stratégies d'intégration des droits humains aux affaires courantes des entreprises, Volume 2, par Craig Forcese, 1997.
Les droits humains : le chaînon manquant de l'APEC, 1997.

Droits et Démocratie

Centre international des droits de la personne
et du développement démocratique

1001, boul. de Maisonneuve Est, Bureau 1100 > Montréal (Québec) H2L 4P9
Tel. : 1 (514) 283-6073 > Telec. : 1 (514) 283-3792 > Courriel : ichrdd@ichrdd.ca > Site Web : www.ichrdd.ca